Adam Rogala-Lewicki

REFORMY SYSTEMU OCHRONY DANYCH OSOBOWYCH W POLSCE W LATACH 1997–2018 ORAZ NA MOCY ROZPORZĄDZENIA PE I RADY (UE) 2016/679 (RODO) – proces, ewolucja systemu, przegląd wybranych zmian, motywy społeczne, praktyka dokumentacyjna

Tom II

WYTYCZNE, ZALECENIA, OPINIE, OŚWIADCZENIA, SPRAWOZDANIA EUROPEJSKIEJ RADY OCHRONY DANYCH (ROZPORZĄDZENIE PE I RADY UE 2016/679) ORAZ GRUPY ROBOCZEJ ART. 29 (DYREKTYWA PE I RADY UE 95/46/WE) – DOKUMENTY ZEBRANE

KUTNO 2022

REFORMY SYSTEMU OCHRONY DANYCH OSOBOWYCH W POLSCE W LATACH 1997–2018 ORAZ NA MOCY ROZPORZĄDZENIA PE I RADY (UE) 2016/679 (RODO) – proces, ewolucja systemu, przegląd wybranych zmian, motywy społeczne, praktyka dokumentacyjna

Adam Rogala-Lewicki

Recenzja wydawnicza:
dr hab. Dominika Narożna
dr hab. Zbigniew Białobłocki

Druk i oprawa
Mazowieckie Centrum Poligrafii
ul. Ciurlionisa 4, 05–270 Marki

Skład i projekt okładki
Łukasz Różyński

Kutno 2022 Wydanie 1

ISBN 978-83-63484-62-0

Wszystkie prawa zastrzeżone © 2022 Akademia Nauk Stosowanych Gospodarki Krajowej w Kutnie

Indeks[1] zebranych wytycznych, zaleceń, opinii, oświadczeń, sprawozdań, dokumentów Europejskiej Rady Ochrony Danych [rozporządzenie PE i Rady (UE) 2016/679[2]] oraz Grupy Roboczej art. 29 [dyrektywa PE i Rady (UE) 95/46/WE[3]] – wybór własny

Wytyczne, zalecenia, opinie, oświadczenia, sprawozdania, dokumenty robocze, noty informacyjne Europejskiej Rady Ochrony Danych

Wytyczne 5/2021 w sprawie wzajemnych relacji pomiędzy stosowaniem art. 3 i przepisami dotyczącymi międzynarodowego przekazywania danych zawartymi w rozdziale V RODO, wersja do konsultacji publicznych, przyjęte 18 listopada 2021r., Europejska Rada Ochrony Danych

Wytyczne 4/2021 w sprawie kodeksów postępowania jako narzędzia do przekazywania danych, wersja do konsultacji publicznych, przyjęte 7 lipca 2021r., Europejska Rada Ochrony Danych

Wytyczne 3/2021 w sprawie stosowania art. 65 ust.1 lit. a) RODO, przyjęte 13 kwietnia 2021r., Europejska Rada Ochrony Danych

Wytyczne 2/2021 w sprawie wirtualnych asystentów głosowych, wersja 2.0, przyjęte 7 lipca 2021r., Europejska Rada Ochrony Danych

Wytyczne 1/2021 w sprawie przykładów dotyczących zgłaszania naruszeń ochrony danych, przyjęte 14 stycznia 2021r., Europejska Rada Ochrony Danych

Wytyczne 10/2020 w sprawie ograniczeń praw osób, których dane dotyczą, na podstawie art. 23 RODO, wersja 2.0. przyjęte 13 października 2021., Europejska Rada Ochrony Danych

Wytyczne 9/2020 w sprawie pojęcia mającego znaczenie dla sprawy i uzasadnionego sprzeciwu, wersja 2.0, przyjęte 9 marca 2021 r., Europejska Rada Ochrony Danych

Wytyczne 8/2020 w sprawie targetowania użytkowników mediów społecznościowych, wersja 2.0, przyjęte 13 kwietnia 2021 r., Europejska Rada Ochrony Danych

Wytyczne 7/2020 w sprawie pojęć administratora i podmiotu przetwarzającego na gruncie RODO, wersja 2.0, przyjęte 7 lipca 2021 r., Europejska Rada Ochrony Danych

Wytyczne 6/2020 w sprawie współzależności pomiędzy dyrektywą PSD2 a RODO, wersja 2.0, przyjęte 15 grudnia 2020 r., Europejska Rada Ochrony Danych

---

[1] Zebrane wytyczne, zalecenia, opinie, oświadczenia, sprawozdania, dokumenty są dostępne w domenie publicznej, w tym na oficjalnej stronie Prezesa Urzędu Ochrony Danych Osobowych: https://uodo.gov.pl/pl/p/prawo.

[2] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz.Urz. UE L 119 z dn. 4.05.2016, s. 1–88).

[3] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych (Dz. Urz. UE L 281 z 23.11.1995, s. 31–50).

Wytyczne 5/2020 w sprawie zgody na mocy rozporządzenia 2016/679, wersja 1.1, przyjęte 4 maja 2020 r., Europejska Rada Ochrony Danych

Wytyczne 04/2020 w sprawie wykorzystywania danych o lokalizacji oraz narzędzi służących ustalaniu kontaktów zakaźnych w kontekście pandemii COVID-19, przyjęte 21 kwietnia 2020 r., Europejska Rada Ochrony Danych

Wytyczne 03/2020 w sprawie przetwarzania danych dotyczących zdrowia do celów badań naukowych w kontekście pandemii COVID-19, przyjęte 21 kwietnia 2020 r., Europejska Rada Ochrony Danych

Wytyczne 2/2020 w sprawie art. 46 ust. 2 lit. a) i art. 46 ust. 3 lit. b) rozporządzenia 2016/679 dotyczącego przekazywania danych osobowych między organami i podmiotami publicznymi z EOG i spoza EOG, wersja 2.0, przyjęte 15 grudnia 2020 r., Europejska Rada Ochrony Danych

Wytyczne 1/2020 w sprawie pojazdów połączonych i aplikacji związanych z mobilnością wersja 2.0, przyjęte 9 marca 2021 r., Europejska Rada Ochrony Danych

Wytyczne 5/2019 w sprawie kryteriów dotyczących prawa do bycia zapomnianym w sprawach dotyczących wyszukiwarek internetowych na podstawie RODO (część 1), wersja 2.0, przyjęte 7 lipca 2020 r., Europejska Rada Ochrony Danych

Wytyczne nr 4/2019 dotyczące artykułu 25. Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych, wersja 2.0, przyjęte 20 października 2020 r., Europejska Rada Ochrony Danych

Wytyczne 3/2019 w sprawie przetwarzania danych osobowych za pomocą urządzeń wideo, wersja 2.0, przyjęte 29 stycznia 2020 r., Europejska Rada Ochrony Danych

Wytyczne 2/2019 w sprawie przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. b) RODO, wersja 2.0, przyjęte 8 października 2019 r., Europejska Rada Ochrony Danych

Wytyczne 1/2019 dotyczące kodeksów postępowania i podmiotów monitorujących zgodnie z RODO, wersja 2.0, przyjęte 4 czerwca 2019 r., Europejska Rada Ochrony Danych

Wytyczne 4/2018 w sprawie akredytacji podmiotów certyfikujących na podstawie artykułu 43 RODO, wersja 3.0, przyjęte 4 czerwca 2019 r., Europejska Rada Ochrony Danych

Wytyczne 3/2018 w sprawie terytorialnego zakresu stosowania RODO (artykuł 3), wersja 2.0, przyjęte 12 listopada 2019 r., Europejska Rada Ochrony Danych

Wytyczne 2/2018 w sprawie wyjątków określonych w art. 49 rozporządzenia 2016/679, przyjęte 25 maja 2018 r., Europejska Rada Ochrony Danych

Wytyczne 1/2018 ws. certyfikacji i określenia kryteriów certyfikacji zgodnie z art. 42 i 43 RODO, wersja 3.0, przyjęte 4 czerwca 2019 r., Europejska Rada Ochrony Danych

Zalecenia 02/2021 w sprawie podstawy prawnej przechowywania danych kart kredytowych w celu ułatwienia dalszych transakcji online, przyjęte 19 maja 2021 r., Europejska Rada Ochrony Danych

Zalecenia 01/2021 w sprawie odpowiedniego stopnia ochrony przekazywanych danych osobowych na mocy dyrektywy 2016/680, przyjęte 2 lutego 2021 r., Europejska Rada Ochrony Danych

Zalecenia 2/2020 w sprawie niezbędnych gwarancji europejskich dla środków nadzoru, przyjęte 10 listopada 2020 r., Europejska Rada Ochrony Danych

Zalecenia 01/2020 dotyczące środków uzupełniających narzędzia przekazywania w celu zapewnienia zgodności z unijnym stopniem ochrony danych osobowych, przyjęte 10 listopada 2020 r., Europejska Rada Ochrony Danych

Zalecenie 01/2019 w sprawie projektu wykazu sporządzonego przez Europejskiego Inspektora Ochrony Danych dotyczącego rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych (art. 39 ust. 4 rozporządzenia (UE) 2018/1725), przyjęte 10 lipca 2019 r., Europejska Rada Ochrony Danych

Wspólna Opinia EROD i EIOD 3/2021 w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie europejskiego zarządzania danymi (akt w sprawie zarządzania danymi), przyjęta 10 marca 2021 r., Europejska Rada Ochrony Danych, Europejski Inspektor Ochrony Danych

Wspólna opinia EROD i EIOD 2/2021 dotycząca decyzji wykonawczej Komisji Europejskiej w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich w zakresie kwestii, o których mowa w art. 46 ust. 2 lit c) rozporządzenia (UE) 2016/679, przyjęta 14 stycznia 2021 r., Europejska Rada Ochrony Danych, Europejski Inspektor Ochrony Danych

Wspólna opinia EROD i EIOD 1/2021 dotycząca decyzji wykonawczej Komisji Europejskiej w sprawie standardowych klauzul umownych między administratorami a podmiotami przetwarzającymi dotyczących kwestii, o których mowa w art. 28 ust. 7 rozporządzenia (UE) 2016/679 i art. 29 ust. 7 rozporządzenia (UE) 2018/1725, przyjęta 14 stycznia 2021 r., Europejska Rada Ochrony Danych, Europejski Inspektor Ochrony Danych

Opinia 18/2021 w sprawie projektu standardowych klauzul umownych przedłożona przez litewski organ nadzorczy (art. 28 ust. 8 RODO), przyjęta 19 maja 2021 r., Europejska Rada Ochrony Danych

Opinia 17/2021 w sprawie projektu decyzji francuskiego organu nadzorczego dotyczącej europejskiego kodeksu postępowania przedłożonego przez Dostawców Usług Infrastruktury Chmury (CISPE), przyjęta 19 maja 2021 r., Europejska Rada Ochrony Danych

Opinia 16/2021 w sprawie projektu decyzji belgijskiego organu nadzorczego dotyczącej „Unijnego kodeksu postępowania ochrony danych dla dostawców usług w chmurze" przedłożonego przez Scope Europe, przyjęta 19 maja 2021 r., Europejska Rada Ochrony Danych

Opinia 15/2021 dotycząca projektu decyzji wykonawczej Komisji Europejskiej na mocy dyrektywy 2016/680 w sprawie stwierdzenia odpowiedniego stopnia ochrony danych osobowych w Zjednoczonym Królestwie, przyjęta 13 kwietnia 2021 r., Europejska Rada Ochrony Danych

Opinia 14/2021 dotycząca projektu decyzji wykonawczej Komisji Europejskiej na mocy rozporządzenia 2016/679 w sprawie stwierdzenia odpowiedniego stopnia ochrony danych osobowych w Zjednoczonym Królestwie, przyjęta 13 kwietnia 2021 r., Europejska Rada Ochrony Danych

Opinia nr 3/2019 w sprawie pytań i odpowiedzi dotyczących wzajemnych zależności między rozporządzeniem w sprawie badań klinicznych (RBK) a ogólnym rozporządzeniem o ochronie danych (RODO) (art. 70 ust. 1 lit. b), przyjęta 23 stycznia 2019 r., Europejska Rada Ochrony Danych

Opinia 28/2018 dotycząca projektu decyzji Komisji Europejskiej stwierdzającej odpowiedni stopień ochrony danych osobowych w Japonii, przyjęta 5 grudnia 2018 r., Europejska Rada Ochrony Danych

Opinia 23/2018 w sprawie wniosków Komisji dotyczących europejskiego nakazu wydania dowodów i europejskiego nakazu zabezpieczenia dowodów w sprawach karnych (art. 70 ust. 1 lit. b), przyjęta 26 września 2018 r., Europejska Rada Ochrony Danych

Oświadczenie w sprawie pakietu usług cyfrowych i strategii i w zakresie danych, przyjęte 18 listopada 2021 r., Europejska Rada Ochrony Danych

Oświadczenie 5/2021 dotyczące rozporządzenia w sprawie zarządzania danymi w świetle zmian legislacyjnych, przyjęte 19 maja 2021 r., Europejska Rada Ochrony Danych

Oświadczenie 4/2021 w sprawie umów międzynarodowych obejmujących przekazywanie danych, przyjęte 13 kwietnia 2021 r., Europejska Rada Ochrony Danych

Oświadczenie 2/2021 w sprawie nowych postanowień Konwencji Rady Europy o cyberprzestępczości (Konwencja Budapeszteńska), przyjęte 2 lutego 2021r., Europejska Rada Ochrony Danych

Oświadczenie dotyczące końca okresu przejściowego Brexit, przyjęte 15 grudnia 2020r., Europejska Rada Ochrony Danych

Oświadczenie w sprawie ochrony danych osobowych przetwarzanych w związku z zapobieganiem praniu pieniędzy i finansowaniu terroryzmu, przyjęte 15 grudnia 2020r., Europejska Rada Ochrony Danych

Oświadczenie w sprawie przyszłego rozporządzenia o prywatności i łączności elektronicznej oraz przyszłej roli organów nadzorczych i EROD w tym kontekście, przyjęte 19 listopada 2020 r., Europejska Rada Ochrony Danych

Oświadczenie 2/2019 w sprawie wykorzystywania danych osobowych w ramach kampanii politycznych wraz z załącznikiem, przyjęte 13 marca 2019 r., Europejska Rada Ochrony Danych

Oświadczenie 01/2019 w sprawie amerykańskiej ustawy o wypełnianiu obowiązków podatkowych w stosunku do rachunków posiadanych za granicą (Foreign Account Tax Compliance Act; FATCA), przyjęte 25 lutego 2019 r., Europejska Rada Ochrony Danych

Oświadczenie w sprawie wpływu koncentracji gospodarczych na ochronę danych, przyjęte 27 sierpnia 2018 r., Europejska Rada Ochrony Danych

Oświadczenie dotyczące zmiany rozporządzenia w sprawie prywatności i łączności elektronicznej oraz jego wpływu na ochronę osób fizycznych w zakresie prywatności i poufności komunikacji, przyjęte 25 maja 2018 r., Europejska Rada Ochrony Danych

Dokument roboczy dotyczący zakresu uprawnień grupy ekspertów wspierających EROD, przyjęty 15 grudnia 2020 r., Europejska Rada Ochrony Danych

Dokument roboczy w sprawie ram skoordynowanego egzekwowania prawa na mocy rozporządzenia 2016/679, przyjęty 20 września 2020 r., Europejska Rada Ochrony Danych

Sprawozdanie EROD dla LIBE (Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych Parlamentu Europejskiego) dotyczące wdrożenia RODO, przyjęte 26 lutego 2019 r., Europejska Rada Ochrony Danych

Wkład EROD do konsultacji w sprawie projektu drugiego protokołu dodatkowego do Konwencji Rady Europy o cyberprzestępczości, przyjęty 13 listopada 2019 r., Europejska Rada Ochrony Danych

Wystąpienie EROD przed TSUE w sprawie C-311/18 (Facebook Ireland i Schrems), przyjęte 9 lipca 2019 r., Europejska Rada Ochrony Danych

Nota informacyjna w sprawie przekazywania danych na mocy RODO do Zjednoczonego Królestwa po zakończeniu okresu przejściowego, przyjęte 15 grudnia 2020 r., Europejska Rada Ochrony Danych

Nota informacyjna w sprawie wiążących reguł korporacyjnych (Binding Corporate Rules, BCR) dla przedsiębiorstw, dla których wiodącym organem nadzorczym jest Urząd Rzecznika Informacji (Information Commissioner's Office, ICO), przyjęta 12 lutego 2019r., Europejska Rada Ochrony Danych

Nota informacyjna dotycząca przekazywania danych osobowych na podstawie ogólnego rozporządzenia o ochronie danych w przypadku braku porozumienia w sprawie Brexitu, przyjęta 12 lutego 2019 r., Europejska Rada Ochrony Danych

Tarcza prywatności UE-USA – Sprawozdanie z drugiego rocznego wspólnego przeglądu, przyjęte 22 stycznia 2019 r., Europejska Rada Ochrony Danych

Tarcza prywatności UE-USA – Sprawozdanie z trzeciego rocznego wspólnego przeglądu, przyjęte 12 listopada 2019 r., Europejska Rada Ochrony Danych

Strategia Europejskiej Rady Ochrony Danych na lata 2021–2023, przyjęta 15 grudnia 2020r., Europejska Rada Ochrony Danych

Wytyczne, zalecenia, opinie, dokumenty robocze Grupy Roboczej art. 29

Wytyczne dotyczące zgody na mocy rozporządzenia 2016/679, przyjęte 28 listopada 2017 r., zmienione i przyjęte 10 kwietnia 2018 r., 17/PL WP259 rev.01, Grupa Robocza art. 29

Wytyczne w sprawie przejrzystości na podstawie rozporządzenia 2016/679, przyjęte 29 listopada 2017 r., zmienione i przyjęte 11 kwietnia 2018 r., WP260 rev.01, Grupa Robocza art. 29

Wytyczne w sprawie zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania do celów rozporządzenia 2016/679/UE, przyjęte 3 października 2017 r., zmienione i przyjęte 6 lutego 2018 r., WP251rev.01, Grupa Robocza art. 29

Wytyczne dotyczące zgłaszania naruszeń ochrony danych osobowych zgodnie z rozporządzeniem 2016/679, przyjęte 3 października 2017 r., zmienione i przyjęte 6 lutego 2018 r. WP250 rev.01, Grupa Robocza art. 29

Wytyczne w sprawie stosowania i ustalania administracyjnych kar pieniężnych do celów rozporządzenia nr 2016/679, przyjęte 3 października 2017 r., WP 253, Grupa Robocza art. 29

Wytyczne dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko" do celów rozporządzenia 2016/679, przyjęte 4 kwietnia 2017 r., zmienione i przyjęte 4 października 2017 r., WP248 rev.01, Grupa Robocza art. 29

Wytyczne dotyczące prawa do przenoszenia danych 2016/679 z załącznikiem, przyjęte 13 grudnia 2016 r., zmienione i przyjęte 5 kwietnia 2017 r., WP242 rev.01, Grupa Robocza art. 29

Wytyczne dotyczące inspektorów ochrony danych, przyjęte 13 grudnia 2016 r., zmienione i przyjęte 5 kwietnia 2017 r., WP243 rev.01, Grupa Robocza art. 29

Wytyczne dotyczące ustalania wiodącego organu nadzorczego właściwego dla administratora lub podmiotu przetwarzającego z załącznikiem, przyjęte 13 grudnia 2016 r., zmienione i przyjęte 5 kwietnia 2017 r., WP244 rev.01, Grupa Robocza art. 29

Zalecenie dotyczące standardowego wniosku o zatwierdzenie Wiążących Reguł Korporacyjnych dla administratora danych dla celów przekazywania danych osobowych, przyjęte 11 kwietnia 2018 r., WP264, Grupa Robocza art. 29

Zalecenie dotyczące standardowego wniosku o zatwierdzenie Wiążących Reguł Korporacyjnych dla podmiotów przetwarzających dla celów przekazywania danych osobowych, przyjęte 11 kwietnia 2018 r., WP265, Grupa Robocza art. 29

Dokument roboczy przedstawiający stanowisko w sprawie wyjątków od obowiązków prowadzenia rejestru czynności przetwarzania zgodnie z art. 30 ust. 5 RODO, przyjęty 19 kwietnia 2018 r., Grupa Robocza art. 29

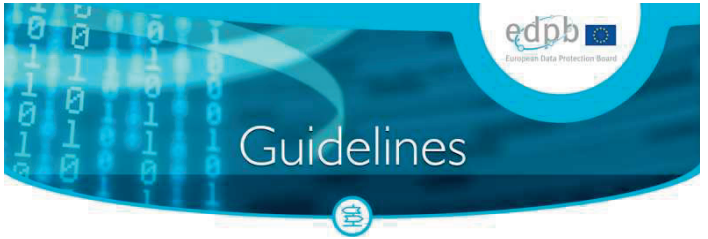
Dokument roboczy ustanawiający procedurę współpracy w celu zatwierdzenia „wiążących reguł korporacyjnych" dla administratorów i podmiotów przetwarzających zgodnie z RODO, przyjęty 11 kwietnia 2018 r., WP263 rev.01, Grupa Robocza art. 29

Dokument roboczy ustanawiający tabelę zawierającą elementy i zasady, które mają zostać uwzględnione w wiążących regułach korporacyjnych dla administratorów, przyjęty 28 listopada 2017 r., zmieniony i przyjęty 6 lutego 2018 r, WP 256 rev.01, Grupa Robocza art. 29

Dokument roboczy ustanawiający tabelę zawierającą elementy i zasady, które mają zostać uwzględnione w wiążących regułach korporacyjnych dla przetwarzających, przyjęty 28 listopada 2017, zmieniony i przyjęty 6 lutego 2018 r., WP 257 rev.01, Grupa Robocza art. 29

Dokument roboczy dotyczący adekwatności (Odpowiedni stopień ochrony przekazywanych danych osobowych), przyjęty 28 listopada 2017 r., zmieniony i przyjęty 6 lutego 2018 r., WP 254rev.01, Grupa Robocza art. 29

* * *



Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR

Adopted on 18 November 2021

Table of contents

1 Introduction 3
2 Criteria to qualify a processing as a transfer of personal data to a third country or to an international organisation 4
2.1 A controller or a processor is subject to the GDPR for the given processing 5
2.2 This controller or processor ("exporter") discloses by transmission or otherwise makes personal data, subject to this processing, available to another controller, joint controller or processor ("importer") 5
2.3 The importer is in a third country or is an international organisation, irrespective of whether or not this importer is subject to the GDPR in respect of the given processing in accordance with Article 3 7
3 Consequences 8

The European Data Protection Board

Having regard to Article 70 (1)(e) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, (hereinafter the "GDPR" or "Regulation"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,[1]

Having regard to Article 12 and Article 22 of its Rules of Procedure,

HAS ADOPTED THE FOLLOWING GUIDELINES:

1 INTRODUCTION

1. According to Article 44of the GDPR,[2] the conditions laid down in its Chapter V shall apply to any "transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation".[3] The overarching purpose of Chapter V is to ensure that the level of protection guaranteed by the GDPR is not undermined when personal data are transferred "to third countries or to international organisations".[4]

2. The provisions of Chapter V aim at ensuring the continued protection of personal data after they have been transferred to a third country or to an international organisation. When personal data is processed on EU territory it is protected not only by the rules in the GDPR but also by other rules, both on EU and Member State level, that must be in line with the GDPR (including possible derogations therein) and ultimately with the EU Charter on fundamental rights and freedoms. When personal data is transferred and made accessible to entities outside the EU territory, the overarching legal framework provided within the Union no longer applies.

3. Therefore, it must be ensured that the transferred personal data is protected in other ways, such as by being transferred in the context of an adequacy decision from the European Commission or by provision of appropriate safeguards in accordance with Chapter V of the GDPR. When relying on one of the transfer tools listed in Article 46 GDPR, it must be assessed whether supplementary measures need to be implemented in order to bring the level of protection of the transferred data up to the EU standard of essential equivalence.[5] This applies also in situations where the processing falls under Article 3(2) of the GDPR, in order to avoid that the protection provided by the GDPR is undermined by other legislation that the importer falls under. This may for example be the case where the third country has rules on government access to personal data that go beyond what is necessary and proportionate in a democratic society (to safeguard one of the important objectives as also recognised in Union or Member States' law, such as those listed in Article 23(1) GDPR). The provisions in Chapter V are there to compensate for this risk and to complement the territorial scope of the GDPR as defined by Article 3 when personal data is transferred to countries outside the EU.

4. The following sections aim at clarifying this interplay between Article 3 and the provisions of the GDPR on international transfers in Chapter V in order to assist controllers and processors in the EU in identifying whether a processing constitutes a transfer to a third country or to an international organisation and, as a result, whether they have to comply with the provisions of Chapter V of the GDPR.

5. It is however important to keep in mind that although a certain data flow may not constitute a transfer under Chapter V, such processing can still be associated with risks for which safeguards must be envisaged. Regardless of whether the processing takes place in the EU or not, controllers and processors always have to comply with all relevant provisions of the GDPR, such as the Article 32 obligation to implement technical and organizational measures taking into account, *inter alia*, the risks with respect to the processing.

2 CRITERIA TO QUALIFY A PROCESSING AS A TRANSFER OF PERSONAL DATA TO A THIRD COUNTRY OR TO AN INTERNATIONAL ORGANISATION

6. Since the GDPR does not provide for a legal definition of the notion "transfer of personal data to a third country or to an international organisation",[6] it is essential to clarify this notion.

7. The EDPB has identified[7] the three following cumulative criteria that qualify a processing as a transfer:

   1) A controller or a processor is subject to the GDPR for the given processing.

   2) This controller or processor ("exporter") discloses by transmission or otherwise makes personal data, subject to this processing, available to another controller, joint controller or processor ("importer").

   3) The importer is in a third country or is an international organisation, irrespective of whether or not this importer is subject to the GDPR in respect of the given processing in accordance with Article 3.

[1] References to "EU" and "Member States" made throughout this document should be understood as references to "EEA" and "EEA Member States" respectively.
[2] "Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation."
[3] "International organisation" means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.
[4] Besides Recital 101, this is particularly emphasized by Article 44, sentence 2 which reads: "All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined."
[5] See EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data and EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures.
[6] Article 44, sentence 1.
[7] Having regard to relevant findings in the CJEU Judgment of 6 November 2003, Bodil Lindqvist, C-101/01, EU:C:2003:596.

8. It is useful to recall here that pursuant to Article 3, the application of the GDPR must always be assessed in relation to a certain processing rather than with regard to a specific entity (e.g. a company).[8]

2.1 A controller or a processor is subject to the GDPR for the given processing

9. The first criterion requires that the processing at stake meets the requirements of Article 3 GDPR, i.e. that a controller or processor is subject to the GDPR for the given processing. This has been further elaborated on in the EDPB Guidelines 3/2018 on the territorial scope of the GDPR (Article 3).

10. It is worth underlining that controllers and processors, which are not established in the EU, may be subject to the GDPR pursuant to Article 3(2) for a given processing and, thus, will have to comply with Chapter V when transferring personal data to a third country or to an international organisation.

2.2 This controller or processor ("exporter") discloses by transmission or otherwise makes personal data, subject to this processing, available to another controller, joint controller or processor ("importer")

11. The second criterion requires that there is a controller or processor disclosing by transmission or otherwise making data available to another controller or processor. These concepts have been further elaborated on in the EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR. It should, *inter alia*, be kept in mind that the concepts of controller, joint controller and processor are *functional* concepts in that they aim to allocate responsibilities according to the actual roles of the parties and *autonomous* concepts in the sense that they should be interpreted mainly according to EU data protection law. A case-by-case analysis of the processing at stake and the roles of the actors involved is necessary.[9]

12. This second criterion cannot be considered as fulfilled where the data are disclosed directly and on his/her own initiative by the data subject[10] to the recipient. In such case, there is no controller or processor sending or making the data available ("exporter").[11]

Example 1: Controller in a third country collects data directly from a data subject in the EU

Maria, living in Italy, inserts her personal data by filling a form on an online clothing website in order to complete her order and receive the dress she bought online at her residence in Rome. The online clothing website is operated by a company established in Singapore with no presence in the EU. In this case, the data subject (Maria) passes her personal data to the Singaporean company, but this does not constitute a transfer of personal data since the data are not passed by an exporter (controller or processor), since they are passed directly and on her own initiative by the data subject herself. Thus, Chapter V does not apply to this case. Nevertheless, the Singaporean company will need to check whether its processing operations are subject to the GDPR pursuant to Article 3(2).[12]

[8] See Sections 1–3 of the EDPB Guidelines 3/2018 on the territorial scope of the GDPR (Article 3).
[9] See page 9 of the EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR.
[10] The data subject cannot be considered a controller or processor. This follows from Article 4(10) GDPR which differentiates between controller/processor and data subject. Hence, a data subject disclosing his/her own personal data cannot be considered an "exporter". This is without prejudice to the fact that a natural person/an individual can be a controller/processor in accordance with Article 4(7) and 4(8) GDPR (e.g. as a self-employed person). However, this does not limit the protection that natural persons acting as a controller/processor enjoy where their own personal data are concerned.
[11] In addition, it is important to recall that where the processing of personal data is carried out "by a natural person in the course of a purely personal or household activity", such processing will, in accordance with Article 2(2)(c), fall outside the material scope of the GDPR.

Example 2: Controller in the EU sends data to a processor in a third country

Company X established in Austria, acting as controller, provides personal data of its employees or customers to a company Z established in Chile, which processes these data as processor on behalf of X. In this case, data are provided from a controller which, as regards the processing in question, is subject to the GDPR, to a processor in a third country. Hence, the provision of data will be considered as a transfer of personal data to a third country and therefore Chapter V of the GDPR applies.

13. It is also important to note that Article 44 of the GDPR clearly envisages that a transfer may not only be carried out by a controller but also by a processor. Therefore, there may be a transfer situation where a processor sends data to another processor or even to a controller as instructed by its controller.

Example 3: Processor in the EU sends data back to its controller in a third country

XYZ Inc., a controller without an EU establishment, sends personal data of its employees/customers, all of them non-EU residents, to the processor ABC Ltd. for processing in the EU, on behalf of XYZ. ABC re-transmits the data to XYZ. The processing performed by ABC, the processor, is covered by the GDPR for processor specific obligations pursuant to Article 3(1), since ABC is established in the EU. Since XYZ is a controller in a third country, the disclosure of data from ABC to XYZ is regarded as a transfer of personal data and therefore Chapter V applies.

Example 4: Processor in the EU sends data to a sub-processor in a third country

Company A established in Germany, acting as controller, has engaged B, a French company, as a processor on its behalf. B wishes to further delegate a part of the processing activities that it is carrying out on behalf of A to sub-processor C, a company established in India, and hence to send the data for this purpose to C. The processing performed by both A and its processor B is carried out in the context of their establishments in the EU and is therefore subject to the GDPR pursuant to its Article 3(1), while the processing by C is carried out in a third country. Hence, the passing of data from processor B to sub-processor C is a transfer to a third country, and Chapter V of the GDPR applies.

14. The second criterion implies that the concept of "transfer of personal data to a third country or to an international organisation" only applies to disclosures of personal data where two different (separate) parties (each of them a controller, joint controller or processor) are involved. In order to qualify as a transfer, there must be a controller or processor disclosing the data (the exporter) and a different controller or processor receiving or being given access to the data (the importer).

Example 5: Employee of a controller in the EU travels to a third country on a business trip

George, employee of A, a company based in Poland, travels to India for a meeting. During his stay in India, George turns on his computer and accesses remotely personal data on his company's databases to finish a memo. This remote access of personal data from a third country, does not qualify as a

[12] In this regard, see Recital 23, which includes elements to be assessed when determining whether the targeting criterion in Article 3(2)(a) GDPR is met.

transfer of personal data, since George is not another controller, but an employee, and thus an integral part of the controller (company A). Therefore, the disclosure is carried out within the same controller (A). The processing, including the remote access and the processing activities carried out by George after the access, are performed by the Polish company, i.e. a controller established in the Union subject to Article 3(1) of the GDPR.

15. Hence, if the sender and the recipient are not different controllers/processors, the disclosure of personal data should not be regarded as a transfer under Chapter V of the GDPR – since data is processed within the same controller/processor. In this context, it should be kept in mind that controllers and processors are nevertheless obliged to implement technical and organisational measures, considering the risks with respect to their processing activities, in accordance with Article 32 of the GDPR.

16. It should also be recalled that entities which form part of the same corporate group may qualify as separate controllers or processors. Consequently, data disclosures between entities belonging to the same corporate group (intra-group data disclosures) may constitute transfers of personal data.

Example 6: A subsidiary (controller) in the EU shares data with its parent company (processor) in a third country

The Irish Company A, which is a subsidiary of the U.S. parent Company B, discloses personal data of its employees to Company B to be stored in a centralized HR database by the parent company in the U.S. In this case the Irish Company A processes (and discloses) the data in its capacity of employer and hence as a controller, while the parent company is a processor. Company A is subject to the GDPR pursuant to Article 3(1) for this processing and Company B is situated in a third country. The disclosure therefore qualifies as a transfer to a third country within the meaning of Chapter V of the GDPR.

17. Although a certain data flow may not qualify as a "transfer" to a third country in accordance with Chapter V of the GDPR, including example 5, such processing can still be associated with risks, for example due to conflicting national laws or government access in a third country as well as difficulties to enforce and obtain redress against entities outside the EU. The controller is accountable for its processing activities, regardless of where they take place, and must comply with the GDPR, including Article 24 ("Responsibility of the controller"), 32 ("Security of processing"), 33 ("Notification of a personal data breach"), 35 ("Data Protection Impact Assessment"), 48 ("Transfers or disclosures not authorised by Union law"), etc. Following from its obligation to implement technical and organisational measures taking into account, *inter alia*, the risks with respect to the processing under Article 32 of the GDPR, a controller may very well conclude that extensive security measures are needed – or even that it would not be lawful – to conduct or proceed with a specific processing operation in a third country although there is no "transfer" situation. For example, a controller may conclude that employees cannot bring their laptops, etc. to certain third countries.

2.3 The importer is in a third country or is an international organisation, irrespective of whether or not this importer is subject to the GDPR in respect of the given processing in accordance with Article 3

18. The third criterion requires that the importer is geographically in a third country or is an international organisation, but regardless of whether the processing at hand falls under the scope of the GDPR.

Example 7: Processor in the EU sends data back to its controller in a third country

Company A, a controller without an EU establishment, offers goods and services to the EU market. The French company B, is processing personal data on behalf of company A. B re-transmits the data to A. The processing performed by the processor B is covered by the GDPR for processor specific obligations pursuant to Article 3(1), since it takes place in the context of the activities of its establishment in the EU. The processing performed by A is also covered by the GDPR, since Article 3(2) applies to A. However, since A is in a third country, the disclosure of data from B to A is regarded as a transfer to a third country and therefore Chapter V applies.

3 CONSEQUENCES

19. If all of the criteria as identified by the EDPB are met, there is a "transfer to a third country or to an international organisation". Thus, a transfer implies that personal data are sent or made available by a controller or processor (exporter) which, regarding the given processing, is subject to the GDPR pursuant to Article 3, to a different controller or processor (importer) in a third country, regardless of whether or not this importer is subject to the GDPR in respect of the given processing.

20. As a consequence, the controller or processor in a "transfer" situation (according to the criteria described above) needs to comply with the conditions of Chapter V and frame the transfer by using the instruments which aim at protecting personal data after they have been transferred to a third country or an international organisation.

21. These instruments include the recognition of the existence of an adequate level of protection in the third country or international organisation to which the data is transferred (Article 45) or, in the absence of such adequate level of protection, the implementation by the exporter (controller or processor) of appropriate safeguards as provided for in Article 46.[13] According to Article 49, personal data can be transferred to a third country or an international organisation without the existence of an adequate level of protection or the implementation of appropriate safeguards only in specific situations and under certain conditions.

22. The main types of transfer tools listed in Article 46 are:

- Standard Contractual Clauses (SCCs).
- Binding Corporate Rules (BCRs).
- Codes of conduct.
- Certification mechanisms.
- Ad hoc contractual clauses.
- International agreements/Administrative arrangements.

23. The content of the safeguards needs to be customized depending on the situation. As an illustration, the guarantees to be provided for a transfer of personal data by a processor are not the same as the

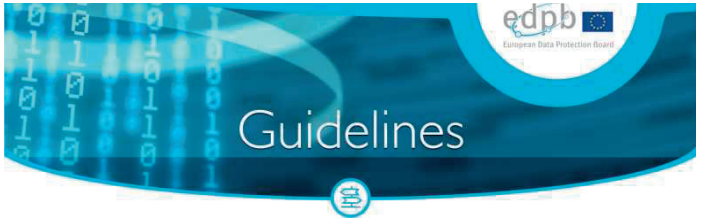
[13] In this context, see also the EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.

ones to be provided for a transfer by a controller.[14] Similarly, for a transfer of personal data to a controller in a third country less protection/safeguards are needed if such controller is already subject to the GDPR for the given processing. Therefore, when developing relevant transfer tools (which currently are only available in theory), i.e. standard contractual clauses or ad hoc contractual clauses, the Article 3(2) situation should be taken into account in order not to duplicate the GDPR obligations but rather to address the elements and principles that are "missing" and, thus, needed to fill the gaps relating to conflicting national laws and government access in the third country as well as the difficulty to enforce and obtain redress against an entity outside the EU. To clarify, such tools should, for example, address the measures to be taken in case of conflict of laws between third country legislation and the GDPR and in the event of third country legally binding requests for disclosure of data. The EDPB encourages and stands ready to cooperate in the development of a transfer tool, such as a new set of standard contractual clauses, in cases where the importer is subject to the GDPR for the given processing in accordance with Article 3(2).

24. To summarize, if the criteria as identified by the EDPB are not met, there is no "transfer" and Chapter V of the GDPR does not apply. As already mentioned, a controller is nonetheless accountable for all processing that it controls, regardless of where it takes place, and data processing in third countries may involve risks which need to be identified and handled (mitigated or eliminated, depending on the circumstances) in order for such processing to be lawful under the GDPR.

25. It is worth underlining that controllers and processors whose processing is subject to the GDPR pursuant to Article 3 always have to comply with Chapter V of the GDPR when they disclose personal data to a controller or processor in a third country or to an international organisation. This also applies to disclosures of personal data carried out by controllers/processors which are not established in the EU but are subject to the GDPR pursuant to Article 3(2) to a controller or processor in the same or another third country.

[14] Cf. Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.



Guidelines 04/2021 on codes of conduct as tools for transfers

Adopted on 07 July 2021

Table of contents

1 AIM OF THE GUIDELINES 3
2 WHAT ARE CODES OF CONDUCT AS A TOOL FOR TRANSFERS? 3
3 WHAT SHOULD BE THE CONTENT OF A CODE OF CONDUCT AS A TOOL FOR TRANSFERS? 5
4 WHO ARE THE ACTORS INVOLVED FOR THE SETTING UP OF A CODE TO BE USED AS A TOOL FOR TRANSFERS AND WHAT IS THEIR ROLE? 7
4.1 Code owner 7
4.2 Monitoring body 7
4.3 SAs 7
4.4 EDPB 8
4.5 EU Commission 8
5 ADOPTION PROCESS OF A CODE OF CONDUCT FOR TRANSFERS 8
6 WHAT ARE THE GUARANTEES TO BE PROVIDED UNDER THE CODE? 9
6.1 Binding and enforceable commitments to be implemented 9
6.2 Check-list of elements to be included in a code of conduct intended for transfers 11
Annex 1 - ADOPTION OF CODE OF CONDUCT FOR TRANSFERS – FLOW CHART 13
a-The draft code is a "transnational code" and/or a code intended for transfers 13
b-The draft code is a "Transnational code" 14

The European Data Protection Board

Having regard to [Article 70 (1)(e) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC], (hereinafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,[1]

Having regard to Article 12 and Article 22 of its Rules of Procedure,

HAS ADOPTED THE FOLLOWING GUIDELINES

1 AIM OF THE GUIDELINES

1. The aim of these guidelines is to specify the application of Article 40-3 of the GDPR relating to codes of conduct as appropriate safeguards for transfers of personal data to third countries in accordance with Article 46-2-e) of the GDPR. They also aim to provide practical guidance including on the content of such codes of conduct, their adoption process and the actors involved as well as the requirements to be met and guarantees to be provided by a code of conduct for transfers.
2. These guidelines should further act as a clear reference for all SAs, the Board and assist the Commission in evaluating codes in a consistent manner and to streamline the procedures involved in the assessment process. They should also provide greater transparency, ensuring that code owners who intend to seek approval for a code of conduct intended to be used as a tool for transfers ("code(s) intended for transfers" hereafter) are fully aware of the process and understand the formal requirements and the appropriate thresholds required for setting up such a code of conduct.
3. The present guidelines complement the EDPB Guidelines 1/2019 on codes of conduct and Monitoring Bodies under Regulation 2016/679 which establish the general framework for the adoption of codes of conduct. The considerations set out in Guidelines 1/2019 notably regarding the admissibility, submission and criteria for approval are thus also valid in the context of the preparation of codes intended for transfers.

2 WHAT ARE CODES OF CONDUCT AS A TOOL FOR TRANSFERS?

4. The GDPR requires in its Article 46 that controllers/processors shall put in place appropriate safeguards for transfers of personal data by to third countries or international organizations.

[1] References to "Member States" made throughout this document should be understood as references to "EEA Member States".

5. To that end, the GDPR diversifies the appropriate safeguards that may be used by organizations under Article 46 for framing transfers to third countries by introducing amongst others, codes of conduct as a new transfer mechanism (articles 40-3 and 46-2-e). In this respect, as provided by Article 40-3, once approved by the competent SA and having been granted general validity within the Union by the Commission, a code of conduct may also be adhered and used by controllers or processors not subject to the GDPR located in third countries for the purpose of providing appropriate safeguards to data transferred to third countries. Such controllers and processors are required to make binding and enforceable commitments, via contractual or other legally binding instruments, to apply the appropriate safeguards provided by the code including with regard to the rights of data subjects as required by Article 40-3.

6. Codes of conduct may be prepared by associations or other bodies representing categories of controllers or processors (code owners) as specified by Article 40-2. As indicated in the EDPB Guidelines 1/2019, a non-exhaustive list of possible code owners would include: trade and representative associations, sectoral organizations, academic organizations and interest groups. According to the same Guidelines, codes intended for transfers could for instance be elaborated by bodies representing a sector (e.g. association/federation from banking and finance, insurance sector) but could also be drawn up for separate sectors which have a common processing activity sharing the same processing characteristics and needs (e.g. HR code drawn up by association/federation of HR professionals, or code on children's data). Such codes would thus allow controllers, processors in third countries, receiving data under the code, to frame these transfers while better addressing the specific processing needs of their sector or common processing activities. As such, they could serve as a more adapted tool compared to other transfer mechanisms that are available under Article 46. Codes of conduct to be used as a tool for transfers will notably allow a given controller or processor in a third country to providing appropriate safeguards for multiple transfers to a third country that are specific to a sector or processing activity. In addition, entities using the codes of conduct do not need to be within the same group to frame their transfers (as is the case for BCRs).

7. It should also be noted that a code intended for transfers adhered by a data importer in a third country can be relied on by controllers/processors subject to the GDPR (i.e. data exporter) for complying with their obligations in case of transfers to third countries in accordance with the GDPR without the need for such controller/processors to adhere to such code themselves. Therefore, a code intended for transfers could frame transfers from controller/processors that do not adhere to that code of conduct to controller/processors in a third country having adhered to that code of conduct, provided that a commitment to comply with the obligations set forth by the code of conduct when processing the transferred data, including with regard to the rights of data subjects, is included in a binding instrument. Groups of companies transferring data from entities subject to the GDPR to those outside of the EEA may also use a code of conduct as a transfer tool where the entities outside the EEA have adhered to that code intended for transfers and have undertaken binding and enforceable commitments related to the transfer. As such, codes intended for transfers may for example be used for framing data flows between organizations not belonging to the same group (e.g. companies in the EEA transferring data to third country organizations operating either in the same or a specific sector) or when a group of companies in a single sector shares data from its entities subject to the GDPR with those outside the EEA.

> **Example n°1**[2]: Company XYZ is headquartered in Italy and has affiliates in Germany, the Netherlands, Spain and Belgium. For the purpose of managing the IT tools used by the group, Company XYZ uses the services of a cloud service provider based in a third country with no presence in the EU. Data processed as part of the use of IT tools involves transfers of data from Company XYZ and its affiliates to the cloud service provider, for the purpose of storage of data. As the cloud service provider in the third country has adhered to a code of conduct to be used as a tool for transfers relating to cloud services approved under article 40-5, data flows from Company XYZ and its affiliates to the cloud service provider can be framed with the code of conduct to which the cloud service provider has adhered. In this case, the use of a code of conduct by the cloud service provider instead of other transfer tools such as BCRs appears more appropriate to the extent that a code of conduct does not require the controller/processor acting as importers to have a presence in the EEA while a presence in the EEA is required for a group of companies for using BCRs. The code of conduct also presents benefits for addressing multiple transfers of data with a single tool compared to (fully) contractual solutions such as SCCs.

8. A code intended for transfers could also frame transfers from controllers/processors subject to the GDPR and controllers/processors in the third country having adhered to the same code of conduct for transfers, provided in any case as explained above that a commitment to comply with the obligations of the code of conduct including with respect to the rights of data subjects is included in a binding instrument.

> **Example n°2**: An association representing categories of controllers/processors involved in the same type of research activities for the health sector and involving regular transfers of data to third country controller/processors develop a code of conduct which is also intended to be used as a tool for transfers. Relevant controllers/processors in the EEA adhere to this code of conduct which is also being adhered by third country controllers/processors. The transfers of data to third country controller/processors as part of the research activities can be framed with this code of conduct.

9. To the extent that it is most likely that codes intended for transfers would be used by relevant entities for framing transfers from more than one Member State and considering that those CoC should have general validity according to Art. 40-9 GDPR, they would as such qualify as "transnational codes" as defined in the Guidelines 1/2019[3].

3 WHAT SHOULD BE THE CONTENT OF A CODE OF CONDUCT AS A TOOL FOR TRANSFERS?

10. As set out above, a code of conduct intended for transfers is one of the tools that can be used by organizations performing particular processing activities - e.g. within a specific sector or a common processing activity which share the same processing characteristics and needs - for providing appropriate safeguards for transfers of personal data to a third country in accordance with Article 46.

[2] The example is without prejudice to EDPB Recommendations 01/2020 on measures that supplement transfer tools

[3] Transnational codes refer to a code which covers processing activities in more than one Member State. See Guidelines 1/2019, Appendix 1 – Distinction between national and transnational codes

11. Also, the provisions of Article 40-3, which refer to the fact that codes intended for transfers may be adhered by controllers/processors not subject to the GDPR under Article 3, suggest that codes intended for transfers are, in part, or as a whole, more specifically designed for third country controllers/processors. Therefore, according to the EDPB, the object of a code intended for transfers should be to set out also the rules that will need to be complied with by the third country controller/processor (the data importer) to ensure that personal data is adequately protected in line with the requirements of Chapter V GDPR when being processed by such third country controller/processor (i.e. data importer).

12. More specifically in terms of content, for the purpose of providing appropriate safeguards in the meaning of Article 46, the following elements need to be addressed:

    - Essential principles, rights and obligations arising under the GDPR for controllers/processors; and
    - Guarantees that are specific to the context of transfers (such as with respect to the issue of onward transfers, conflict of laws in the third country).

13. In this regard, it is worth noting that a code of conduct may originally be drawn up only for the purpose of specifying the application of the GDPR in accordance with Article 40-2 ("GDPR code") or also as a code intended for transfers in accordance with Article 40-3. As a consequence, depending on the original scope and content of the code, it may need to be amended in order to cover all of the above mentioned elements if it is to be used as a tool for transfers.

> **Example n°3**: Association ABC gathering organizations operating in the direct marketing sector at EU level has adopted a code of conduct which aims at specifying the application of the transparency principle and associated requirements under the GDPR as part of the processing activities for such sector. The Association wishes to use this code of conduct as a tool for framing transfers outside the EEA. To the extent that the code of conduct is focused on the transparency principle, it would need to be amended in order to cover additionally the appropriate safeguards that are required for international transfers of personal data, all essential principles and main requirements arising under the GDPR (other than transparency) as well as include guarantees that are specific to the context of transfers in order to obtain approval for such code as a code intended for transfers.

14. In any event, in line with the clarifications provided by the EDPB in its guidelines 1/2019, all elements providing for appropriate safeguards as referred above will need to be set out in the code in a manner that facilitates their effective application and specifies how they apply in practice to the specific processing activity or sector[4].

15. A check-list of the elements to be included in a code intended for transfers so that it can be considered as providing appropriate safeguards is further provided and explained under section 6 of the present guidelines.

[4] See Guidelines 1/2019, section 6

4 WHO ARE THE ACTORS INVOLVED FOR THE SETTING UP OF A CODE TO BE USED AS A TOOL FOR TRANSFERS AND WHAT IS THEIR ROLE?

4.1 Code owner

16. The code owner is the entity, association/federation or other body that will prepare a code of conduct intended for transfers or amend an approved "GDPR code" for using it as a tool for transfers and submit it to the competent supervisory authority for approval[5].

4.2 Monitoring body

17. As for any code of conduct, a monitoring body will need to be identified as part of a code intended for transfers and accredited by the competent SA in line with article 41. More precisely, its role will be to monitor that third country controllers/processors having adhered to such code comply with the rules set out in the code[6].

18. Considering that codes of conduct intended for transfers are also or more specifically aimed for third country controller/processors, it has to be made sure that monitoring bodies are capable of effectively monitoring the code as specified in the Guidelines 1/2019. Monitoring bodies acting in the framework of codes for transfers could be located either only inside or also outside of the EEA provided that the concerned monitoring body has an establishment in the EEA. In this context, the monitoring body's establishment in the EEA shall be the one where the headquarters of the monitoring body are, or the place where the final decisions concerning monitoring activities are taken and also requires that an EEA entity shall be able to control the monitoring body's entities outside the EEA and demonstrate full accountability for all decisions and actions (including its liability for any breaches). In addition, a monitoring body in the EEA may subcontract its activities to an external entity outside the EEA, acting on its behalf, provided that such entity maintains the same competence and expertise as required by the code of conduct as well as by the accreditation requirements, and that the EEA monitoring body is able to ensure effective control over the services provided by the contracting entity and retains the decision making power about monitoring activities.

4.3 SAs

19. In accordance with Article 40-5, the role of the competent Supervisory Authority will be to approve the draft code of conduct intended for transfers or amendment it for using it as a tool for transfers and to accredit the monitoring body identified as part of the code. Where necessary, in the scenario of an amendment to the code of conduct, the SA will accredit the monitoring body, only with respect to additional accreditation requirements relating to codes of conduct for transfers.

[5] For further details on the requirements relating to the code owner, please refer to the definition of code owner in section 2 and section 5.3 of Guidelines 1/2019

[6] For further details on the need to set up a monitoring body under a code of conduct, please refer to sections 11 and 12 of Guidelines 1/2019

4.4 EDPB

20. In accordance with Articles 40-7 and 64-1-b, the EDPB will be asked to provide an opinion on the draft decision of a SA aiming to approve a code intended for transfers or amendment to a code of conduct for using it also as a tool for transfers.

4.5 EU Commission

21. As provided by Article 40-9, the Commission may decide by adopting an implementing act that a code intended for transfers and approved by an SA has general validity within the Union. Only those codes having been granted general validity within the Union may be relied upon for framing transfers.

5 ADOPTION PROCESS OF A CODE OF CONDUCT FOR TRANSFERS

22. It results from Articles 40-5 and 40-9 that to be adopted, a code intended for transfers shall first be approved by a competent SA in the EEA and then recognized by the Commission as having general validity within the Union by way of implementing act.

23. As mentioned in section 2 above, to the extent that codes intended for transfers are most likely to be used by controllers/processors for framing transfers from more than one Member State, they would as such qualify as "transnational codes" and should follow the procedure for approval for transnational codes, including the need for an Opinion from the EDPB, as specified in section 8 and Annex 4 of the Guidelines 1/2019[7]. In practice different scenarios may arise when an association/federation or other body intends to adopt a code of conduct for transfers:

- A draft code is designed as a "GDPR code" as well as intended to be used as a tool for transfers by third country controller/processors. Such draft code would first need to be approved by the competent SA according to the procedure for transnational codes, including an Opinion from the Board, and then recognized by the Commission as having general validity within the Union in accordance with Article 40-9. After completion of these steps, controllers/processors in third country may adhere to the code and the code may be used for providing appropriate safeguards for transfers of data to third countries.
- A code of conduct is initially designed and approved as a "GDPR code". Such code is further expanded in view of being also used as a tool for transfers by third country controller/processors. The amendment to the code relating to transfers will need to be submitted to the competent SA for approval which will follow the procedure for transnational codes involving an Opinion from the Board. The amended code will then need to be recognized by the Commission as having general validity within the Union in accordance with Article 40-9 after which controllers/in third country may adhere to such code and use it for providing appropriate safeguards for transfers of personal data to third countries.

24. A flow chart set out in the annex to the guidelines details the procedural steps for adopting a code of conduct intended for transfer in consideration of the above possible scenarios.

[7] See Guidelines 1/2019, Appendix 1 – Distinction between national and transnational codes

6 WHAT ARE THE GUARANTEES TO BE PROVIDED UNDER THE CODE?

6.1 Binding and enforceable commitments to be implemented

25. The GDPR requires in its article 40-3 that controllers and processors not subject to the GDPR adhering to a code intended for transfers take binding and enforceable commitments, via contractual or other legally binding instruments, to apply the appropriate safeguards provided by the code including with regard to the rights of data subjects.

26. As specified by the GDPR, such commitments may be taken by using a contract, which appears as the most straightforward solution. Other instruments could also be used, provided that these controller/processors adhering to the code are able to demonstrate the binding and enforceable character of such other means.

27. In any event, the instrument needs to have a binding and enforceable nature in accordance with EU law and should also be binding and enforceable by data subjects as third party beneficiaries.

28. A Code of Conduct as a transfer tool can have Code members located in the EEA, as well as Code members located outside the EEA. A distinction between Code members located in the EEA and Code members located outside the EEA is the direct application of the GDPR to the former but not the latter (provided that the latter does not fall under Art 3.2 GDPR).

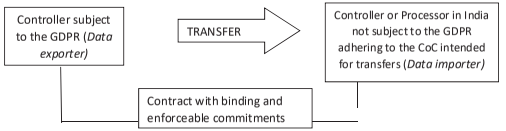
29. In order to ensure that the Code Member's commitment to adhere to a "specified level of data protection" in a particular sector as set in the code of conduct can be effectively met by both types of Code members, there is a need to ensure that the level of data protection provided for in the GDPR is also committed to by these Code members located outside the EEA. This is a prerequisite for their eligibility to participate in the Code of conduct as a transfer tool. Therefore, the 'binding and enforceable commitments' aim to address this discrepancy between these Code members in the EEA and outside the EEA contractually, and ensures that the 'level of data protection' provided for in the GDPR is ensured also by them.

30. To this end, a contract could, for example, be signed by the controller/processor in the third country (i.e. the data importer) with, the entity transferring data under the code (i.e. data exporter). In practice, the parties could use an existing contract if any (e.g. service agreement between the exporter and the data importer or the contract to be put in place in accordance with article 28 GDPR in case of importer-processors) in which the binding and enforceable commitments could be included. Another option could be to rely on a separate contract for instance by adding to the code intended for transfers a model contract that would need to be then signed by controllers/processors in the third country and all of its exporters.

31. Controllers/processors should be able to choose the most appropriate option between the above possibilities depending on their specific situation.

32. When the code of conduct is to be used for transfers and onward transfers by a processor to sub-processors, a reference to the Code of Conduct and the instrument providing for binding and enforceable commitments should also be made in the processor agreement signed between the processor and its controller.

Binding and enforceable commitments with data exporter



33. In general, the contract or other instrument must set out that the controller/processor commits to comply with the rules specified in the code intended for transfers when processing data received under the code. The contract or other instrument shall also provide for mechanisms allowing to enforce such commitments in case of breaches by the controller/processor in particular with respect to the rights of data subjects whose data will be transferred under the code.

34. More particularly, the contract or other instrument should address:

- The existence of a right for data subjects whose data are transferred under the code to enforce the rules under the code as third party beneficiaries;
- The issue of liability in case of breaches to the rules under the code by code member outside of the EEA. The code shall include a jurisdiction clause noting that data subjects, shall have the possibility in case of violation of rules under the code by a code member outside the EEA to bring a claim, by invoking their third-party beneficiary right, including for compensation, against that entity before a EEA SAs and EEA court of the data subject's habitual residence. The code member outside the EEA shall accept the decision of the data subject to do so. Data subjects shall also have the possibility to bring any claim arising out or from the respect by the importer of the code of conduct against the data exporter before the SA or the court of the data exporter's establishment or of the data subject's habitual residence. This liability should be without prejudice to the mechanisms to be implemented under the code with the monitoring body that can also take action against controllers/processors in accordance with the code by imposing corrective measures. The data importer and the data exporter should also accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of the GDPR.
- The existence of a right for the exporter to enforce against the code member the rules under the code as a third-party beneficiary
- The existence of an obligation to notify the exporter and the Supervisory Authority of the data exporter of any detected violation of the code by the code member outside the EEA and of any corrective measures taken by the monitoring body in response to that violation.

6.2 Check-list of elements to be included in a code of conduct intended for transfers

35. In light of safeguards provided by existing transfer tools under article 46 GDPR (such as binding corporate rules), and to ensure consistency in the level of protection, as well as taking into account the CJEU Schrems II ruling[8], the EDPB is of the view that to be considered as providing appropriate safeguards, the elements to be covered by a code of conduct intended for transfers should include the following:

- A description of transfers to be covered by the code (nature of data transferred, categories of data subjects, countries);
- A description of the data protection principles to be complied with under the code (transparency, fairness and lawfulness, purpose limitation, data minimization and accuracy, limited storage of data, processing of sensitive data, security, for processors compliance with instructions from the controller), including rules on using processors or sub-processors and rules on onward transfers;
- Accountability measures to be taken under the code;
- The setting up of an appropriate governance through DPOs or other privacy staff in charge of compliance with data protection obligations resulting from the code;
- The existence of a suitable training program on the obligations arising from the code;
- The existence of a data protection audit (by either internal or external auditors) or other internal mechanism for monitoring compliance with the code, independently from the oversight to be performed by the monitoring body as for any code of conduct; Whereas the aim of the data protection audit program is to ensure and demonstrate compliance with the code, the aim of the audits performed by the monitoring body is to assess whether the applicant is eligible to participate to the code, continues to be eligible once it is a member, and whether sanctions are necessary in case of infringements;
- Transparency measures, including easy access, regarding the use of the code in particular with respect to third party beneficiary rights;
- The provision of data subject rights of information, access, rectification erasure, restriction, notification regarding rectification or erasure or restriction, objection to processing, right not to be subject to decisions based solely on automated processing, including profiling as those provided for by Art. 12, 13, 14, 15, 16, 17, 18, 19, 21, and 22 GDPR;
- The creation of third-party beneficiary rights for data subjects to enforce the rules of the code as third-party beneficiaries (as well as the possibility to lodge a complaint before the competent SA and before EEA Courts;
- The existence of an appropriate complaint handling process maintained by the monitoring body which if deemed appropriate may be complemented with an internal procedure to the code member for managing complaints;
- A warranty that at the time of adhering to the code, the third country controller/processor has no reasons to believe that the laws applicable to the processing of personal data in the third country of transfer, prevent it from fulfilling its obligations under the code and to implement

[8] Judgment of the Court (Grand Chamber) of 16 July 2020; Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems;

where necessary together with the exporter supplementary measures[9] to ensure the required level of protection under EEA law. In addition, a description of the steps to be taken (including notification to the exporter in the EEA, implementation of appropriate supplementary measures) in case after having adhered to the code the third country controller/processor becomes aware of any legislation of the third country preventing compliance by the code member with commitments taken as part of the code and measures to be taken in case of third country government access requests;

- The mechanisms for dealing with changes to the code;
- The consequences of withdrawal of a member from the code;
- A commitment for the code member and monitoring body to cooperate with EEA SAs;
- A commitment for the code member to accept the be subject to the jurisdiction of EEA SAs in any procedure aimed at ensuring compliance with the code of conduct and EEA Courts;
- The criteria of selection of the monitoring body for a code intended for transfers i.e. to demonstrate that the monitoring body has the requisite level of expertise to carry out its role in an effective manner for such a code intended for transfers

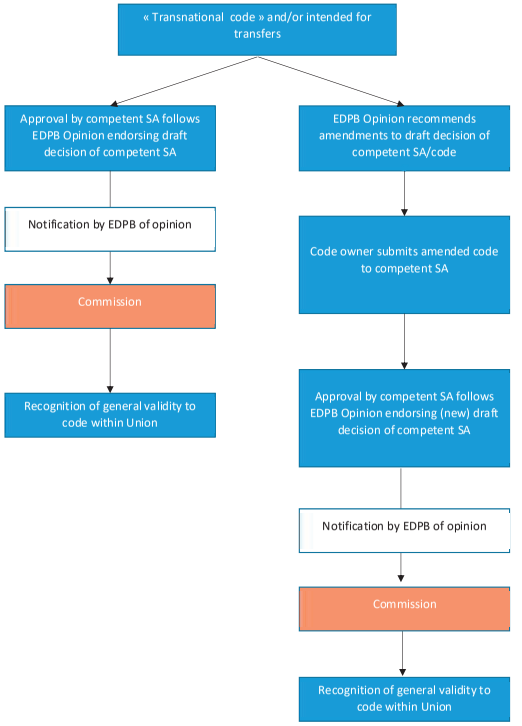
36. In any event, it should be noted that these elements constitute minimum guarantees which may need to be complemented with additional commitments and measures depending on the transfer at stake under the code of conduct.

37. The EDPB will provide further guidance to clarify the application of the above listed elements.

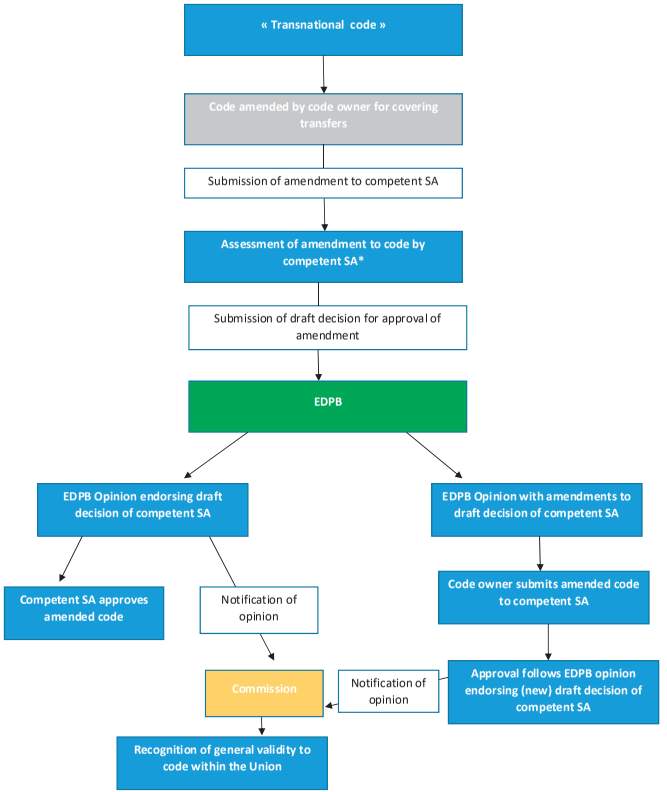
[9] The European Data Protection Board has published a Recommendation on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data which can assist in the assessment relating to the third country and for identifying appropriate supplementary measures.

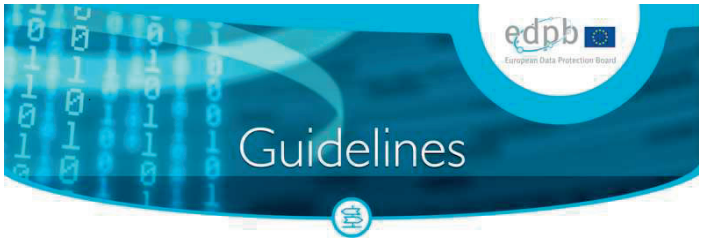
ANNEX 1 - ADOPTION OF CODE OF CONDUCT FOR TRANSFERS – FLOW CHART

a-The draft code is a "transnational code" and/or a code intended for transfers



b-The draft code is a "Transnational code"





Guidelines 03/2021 on the application of Article 65(1)(a) GDPR

Adopted on 13 April 2021

Table of contents

1 Introduction and scope ... 4
2 Legal framework and Rules of Procedure ... 5
2.1 Right to good administration ... 5
2.2 GDPR ... 5
2.3 EDPB Rules of procedure (RoP) ... 6
3 Main stages of the procedure (overview) ... 6
3.1 Conditions for adopting a binding decision ... 6
3.2 Assessment of the completeness of the file ... 7
3.3 Establishment of deadline(s) ... 10
3.3.1 Calculation ... 10
3.3.2 Decision to extend by one month ... 11
3.3.3 Extension by two weeks ... 11
3.4 Preparation of the draft EDPB binding decision ... 11
3.5 Adoption of the EDPB binding decision ... 12
3.6 Notification to the supervisory authorities concerned ... 12
3.7 Final Decision of the supervisory authority(ies) ... 13
3.7.1 "On the basis of" ... 13
3.7.2 Decision(s) by LSA and/or CSA ... 13
3.7.3 Notification of the EDPB ... 14
3.8 Publication of the EDPB binding decision ... 14
4 Competence of the EDPB ... 15
4.1 Assessment of whether the objections are relevant and reasoned ... 15
4.2 Matters subject of the relevant and reasoned objection ... 16
4.2.1 Existence of a given infringement of the GDPR ... 17
4.2.2 Additional or alternative infringements of the GDPR ... 17
4.2.3 Gaps in the draft decision justifying the need for further investigation by the LSA ... 18
4.2.4 Insufficient factual information or reasoning ... 19
4.2.5 Procedural aspects ... 20
4.2.6 Action envisaged ... 21
5 The Right to be heard ... 22
5.1 Applicability ... 22
5.2 Purpose ... 23
5.3 Timing ... 23
5.3.1 At national level and prior to referral to the EDPB ... 23
5.3.2 During the assessment of completeness of the file ... 24
6 Access to the file ... 25
7 The duty to give reasons ... 26
8 Judicial remedies ... 27
8.1 Supervisory authorities ... 28
8.2 Controller, processor, complainant, or other entity ... 29

1 INTRODUCTION AND SCOPE

1. Article 65(1)(a) GDPR requires the EDPB to issue a legally binding decision whenever a Lead Supervisory Authority (LSA) issues a draft decision within the meaning of Article 60(3) GDPR and decides not to follow a relevant and reasoned objection expressed by a Concerned Supervisory Authority (CSA) or is of the opinion that the objection is not relevant or reasoned[1].

2. Article 65(1)(a) GDPR is a **dispute resolution** mechanism meant to ensure the correct and consistent application of the GDPR in cases involving cross-border processing of personal data[2]. It aims to resolve conflicting views among the LSA(s) and CSA(s) on the merits of the case, in particular whether there is an infringement of the GDPR or not, in order to ensure the correct and consistent application of the GDPR in individual cases[3].

3. Under the so-called 'one-stop-shop mechanism', which applies to cross-border processing of personal data, the LSA acts as the sole interlocutor for the controller or processor for the processing at issue[4]. The LSA is responsible for carrying out the necessary investigations, communicating the relevant information to all CSAs and preparing a draft decision[5]. Prior to the adoption of the draft decision, the LSA is required to cooperate with the CSAs in an endeavour to reach consensus and the LSA and CSAs to exchange all relevant information[6].

4. Once a draft decision has been prepared, the LSA shall submit this draft decision to all CSAs for their opinion and take due account of their views[7]. Within four weeks after having been consulted, a CSA can express a "relevant and reasoned objection" to the draft decision[8]. When no CSA objects, the LSA may proceed to adopt the decision. If any CSA expresses an objection, the LSA must decide whether it will follow the relevant and reasoned objection or is of the opinion that the objection is not relevant or reasoned. If the LSA does not intend to follow the objection(s) or considers the objection(s) are not relevant and reasoned, the LSA is obliged to refer the case to the EDPB for dispute resolution[9].

[1] On the concept of relevant an reasoned objection see European Data Protection Board, Guidelines 9/2020 on relevant and reasoned objection under Regulation 2016/679, Version 2.0, 9 March 2021 (hereafter, "RRO Guidelines"), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202009_rro_final_en.pdf.
[2] The cooperation and consistency mechanism is applicable to 'individual cases' regardless of whether the case concerns a complaint or ex officio inquiry/investigation.
[3] Recital (136) and Article 65(1)(a) GDPR.
[4] Article 56(6) GDPR. In cases involving data subject complaint(s), each CSA acts as the main point of contact for the data subject(s) in the territory of its Member State. See Article 60(7)-(9), Article 65(6) and article 77(2) GDPR. See also Recitals (130) and (141) GDPR.
[5] See Article 60(3) GDPR. In accordance with Article 60(2) GDPR, the LSA may request at any time the other CSA to provide mutual assistance pursuant to Article 61 and may conduct joint operations pursuant to Article 62 GDPR.
[6] This duty of cooperation applies to every stage of the procedure, starting with the inception of the case and extending to the whole decision-making process, see Article 60(1) GDPR and RRO Guidelines, paragraph 1. As part of the cooperation procedure, the LSA and CSAs are also required to exchange all relevant information with each other (Article 60(1) GDPR).
[7] Article 60(3) GDPR.
[8] Article 60(4) GDPR.
[9] Articles 60(4), 63 and 65(1)(a) GDPR. If the LSA intends to follow the objection(s) that are deemed relevant and reasoned, it shall submit a revised draft decision to all the CSAs. The CSAs then have a period of two weeks during which they can express their relevant and reasoned objections to the revised draft decision (Article 60(5) GDPR). See also RRO GLS, paragraphs 2-3.
[10] This will apply in particular if the complaint is totally or partially dismissed (Article 60 (8)-(9) GDPR). See further at paragraph 51 and following.
[11] EDPB Rules of Procedure, adopted on 25 May 2018, as last modified and adopted on 8 October 2020, available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_rop_version_7_adopted_20201008_en.pdf (hereafter 'RoP').

5. The EDPB will then act as a dispute resolution body and adopt a **legally binding decision**. The LSA, and in some situations the CSA with which the complaint was lodged[10], must adopt its final decision on the basis of the EDPB decision. The final decision of the competent supervisory authority will be addressed to the controller or processor and, where relevant, to the complainant.

6. These Guidelines clarify the application of Article 65(1)(a) GDPR. In particular, they clarify the application of the relevant provisions of the GDPR and Rules of Procedure, delineate the **main stages** of the procedure and clarify the **competence of the EDPB** when adopting a legally binding decision on the basis of Article 65(1)(a) GDPR. The Guidelines also include a description of the applicable **procedural safeguards and remedies**.

7. The present Guidelines do not concern dispute resolution by the EDPB in cases where:

- there are conflicting views on which of the supervisory authorities concerned is competent for the main establishment (Article 65(1)(b) GDPR);
- a competent supervisory authority does not request the opinion of the Board in the cases referred to in Article 64(1), or does not follow the opinion of the Board issued under Article 64 (Article 65(1)(c) GDPR).

2 LEGAL FRAMEWORK AND RULES OF PROCEDURE

2.1 Right to good administration

8. The EDPB is subject to the Charter of fundamental rights of the European Union (CFEU), including Article 41 (right to good administration). This is also reflected in Article 11(1) EDPB Rules of Procedure[11], which confirms that the EDPB must respect the right to good administration as set out by Article 41 CFEU.

9. Article 41 CFEU grants every person the right to have his or her affairs handled **impartially, fairly and within a reasonable time** by the institutions, bodies, offices and agencies of the Union. This includes the right of every person:

- **to be heard** before any individual measure, which would affect him or her adversely is taken; and
- **to have access** to his or her file, while respecting the legitimate interests of confidentiality and of professional and business secrecy.

The right to good administration also includes the obligation of the administration to **give reasons** for its decisions.

2.2 GDPR

10. Article 65(1) GDPR identifies three different situations in which the EDPB acts as a dispute resolution body. The main rules applicable to the dispute resolution procedures are set out in Article 65(2)-(6) GDPR.

11. In case of a dispute resolution on the basis of Article 65(1)(a) GDPR, regard must also be given to Article 60 GDPR, which applies to the cooperation between the LSA and CSA in individual cases involving cross-border processing and specifies in which cases the LSA submit the matter to the EDPB for dispute resolution. While these Guidelines focus primarily on the application of Article 65(1)(a) GDPR, reference will also be made to the provisions of Article 60 GDPR insofar as they are relevant to clarify the main stages of the procedure and competence of the EDPB under Article 65(1)(a) GDPR.

2.3 EDPB Rules of procedure (RoP)

12. Article 11 RoP further clarifies the rules applicable in cases where the EDPB is called upon to take a binding decision, including in the context of the dispute resolution procedure. Article 11(2) RoP contains rules that apply specifically to the dispute resolution procedure of Article 65(1)(a) GDPR.

13. While not the focus of these Guidelines, regard will also be had to Article 22 (Voting), Article 32 (Access to documents), Article 33 (Confidentiality of discussions) and Article 40 (Calculation of time limits) of the RoP, as appropriate.

3 MAIN STAGES OF THE PROCEDURE (OVERVIEW)

3.1 Conditions for adopting a binding decision

14. The general conditions for the adoption of a binding decision by the EDPB are set forth in Article 60(4)-(5) and Article 65(1)(a) GDPR.

15. The EDPB shall be competent to issue binding decisions on the basis of Article 65(1)(a) GDPR when the following conditions are met:

- the submission of a draft decision within the meaning of Article 60(3) by the LSA to the CSAs;
- at least one CSA has raised (one or more) objection(s) to the (revised) draft decision of the LSA within the deadline provided by Article 60(4)-(5) GDPR; and
- the LSA has decided to not follow the objection(s) on the draft decision or rejected it (them) as not relevant or reasoned.

16. When these conditions are met, the EDPB shall be competent to adopt a binding decision on the basis of Article 65(1)(a) GDPR, which shall concern all the matters which are the subject of the relevant and reasoned objection(s), in particular whether there is an infringement of the GDPR[12].

17. A mere "comment" expressed by a CSA in relation to a draft decision does not amount to an objection within the meaning of Article 4(24) GDPR. The existence of comments shall therefore not give rise to the obligation to trigger the Article 65(1)(a) procedure if the LSA decides not to give any effect to the comment. Moreover, any comment expressed does not constitute as such a matter to be decided by the EDPB as part of its binding decision. The LSA is required, however, to take due account of the views expressed by all CSAs[13] and, in cases where the conditions of Article 56(2) are met, take utmost account of the views expressed by the CSA with whom the complaint has been lodged when preparing the draft decision and take due account of the views expressed by all CSAs[14].

[12] See Section 4 for further details concerning the competence of the EDPB in accordance with Article 65(1)(a) GDPR.

3.2 Assessment of the completeness of the file

18. Article 11(2) RoP provides that the Chair and the LSA are responsible for deciding whether the file is complete[15]. The assessment of the completeness of the file is an important step in the procedure, designed to ensure that all conditions for adopting a binding decision are met and that the EDPB has all the information necessary for doing so[16]. The assessment of completeness of the file also serves as the starting point for the legal deadlines mentioned in Article 65(2)-(3) GDPR[17]. Finally, the assessment of completeness of the file also seeks to ensure compliance with the right to be heard contained in Article 41 CFEU.

19. When submitting the matter to the EDPB for dispute resolution, the LSA shall include:

a) the **draft decision or revised draft decision** subject to the objection(s);

b) a **summary** of the relevant facts and grounds;

c) the **objection(s) made** by the supervisory authority(/-ies) concerned in accordance with Article 60 (4) (and where relevant Article 60(5) GDPR);

d) an **indication** as to whether the LSA **does not follow** the relevant and reasoned objection or is of the opinion that the objection is **not relevant or reasoned**;

e) **documentation proving the timing and format of the provision of the (revised) draft decision and of the objection(s)** by the concerned supervisory authority (/-ies)[18]; and

f) in accordance with Article 41 of the European Charter on Fundamental Rights, the **written observations the LSA collected from the persons that might be adversely affected by the Board's decision**, together with confirmation and evidence of which documents submitted to the Board were provided to them when they were invited to **exercise their right to be heard** or a clear identification of the elements for which it is not the case[19].

20. The wording of Article 60(4) GDPR and Article 11(2) RoP makes clear that the LSA is responsible for ensuring that the file is complete and submitting all relevant information to the EDPB. Where necessary, however, the Secretariat may request from the LSA and/or CSAs additional information within a specific timeframe[20]. The ability to request additional information should be interpreted in light of the objective of ensuring that the EDPB is provided with all information necessary to take a

[13] Article 60(3) GDPR.
[14] Article 56(4) and Article 60(1) GDPR.
[15] The Secretariat carries out the analysis on the completeness of the file on behalf of the Chair.
[16] When necessary, the documents submitted by the competent authority will be translated into English by the EDPB Secretariat.
[17] See Article 11(4) RoP and see further Section 3.3.
[18] The aim of providing this information is to allow the Secretariat to verify the objection has been provided in writing and within the legal deadline. The timing and format of the provision of the (revised) draft decision and of the objection(s) can be proven, for example, via the relevant and reasoned objections report from the information and communication system mentioned in Article 17 of the RoP.
[19] Article 11(2) RoP. See also section 5.
[20] Article 11(2) RoP.

binding decision concerning all the matters which are the subject of the relevant and reasoned objection(s), in particular whether there is an infringement of the GDPR.

Example 1:

A draft decision includes several references to internal documentation of the controller. Even though the LSA's (disputed) finding of an infringement is evidenced in its draft decision with reference to the contents of this documentation, the LSA does not include a copy thereof when submitting the matter to the EDPB for dispute resolution. The Secretariat may request the LSA to provide a copy of the documentation that is referenced within a specific timeframe if needed to help decide the subject matter of the relevant and reasoned objection(s).

The ability to request additional information at a later stage does not diminish the responsibility of the LSA to provide all relevant information from the outset when submitting the matter to the EDPB. As the responsibility for ensuring that the file is complete lies with the LSA, the requesting of additional information from the LSA and/or CSA should in principle only be necessary in exceptional circumstances. Moreover, as the LSA and CSA are obliged to exchange all relevant information in the course of the cooperation procedure, the relevant information should already have been provided to CSAs prior to launching the dispute resolution procedure. If all information necessary to take a binding decision on the objections raised is also transmitted by the LSA when referring the subject matter to the EDPB, it will not be necessary for the Secretariat to request additional information before declaring the file complete.

21. It should be noted that a request for additional information merely seeks to ensure the completeness of the file. It does *not* imply any judgement regarding the merit of the objections raised, nor does it alter in any way the subject matter referred to the EDPB. Once the file is deemed complete and the subject matter is referred to the EDPB, in exceptional circumstances, additional information may also be requested at a later stage in the procedure (i.e. once the subject matter has been referred to the Board) if necessary to remedy any omissions. This will be subject to a decision by the EDPB[21].

22. When necessary, the documents submitted by the LSA and/or CSA will be translated into English by the Secretariat[22]. The translation may also be limited to the specific parts which are likely to be relevant to help decide the subject matter of the relevant and reasoned objection(s). The LSA and/or CSA will have to agree on the translation[23].

Example 2:

In its draft decision, the LSA concludes that only one of the infringements of the GDPR alleged by the complainant materialised. The CSA considers in its relevant and reasoned objection that the other infringements alleged by the complainant were also committed while the draft decision does not fully explain the factual elements necessary to conclude the infringements did not occur. Therefore, the Secretariat requests the LSA to provide a copy of the necessary parts of the investigation report within a specific timeframe[24]. If the translation of these parts is necessary, it will be translated into English by the Secretariat and the LSA will have to agree on the translation.

23. Once the Chair and the LSA have decided that the file is complete (and the competent supervisory authority agreed on any required English translations), the Secretariat on behalf of the Chair will refer the subject-matter to the members of the EDPB without undue delay[25].

24. If the LSA fails to provide the information listed above within the set timeframe[26], the Chair will ask the Secretariat to refer the subject-matter to the EDPB. The EDPB will then assess, on a case-by-case basis, whether it can proceed to adopt its decision on the basis of the information already provided, or whether it is necessary to first obtain the information requested (e.g., confirmation and evidence of which documents submitted to the Board were provided to them when they were invited to exercise their right to be heard or a clear identification of the elements for which it is not the case) before adopting a decision.

Relationship with the right to be heard

25. The assessment of completeness of the file also seeks to ensure compliance with the right to be heard contained in Article 41 CFEU. Article 11(2) RoP provides that the EDPB shall take into account *only* the documents which were provided by the LSA and the other CSA(s) before the matter is referred to the Board. Any person who might be adversely affected should therefore in principle already have been invited to exercise their right to be heard[27]. Where necessary, the Board will take further actions ensuring the right to be heard of the affected persons in relation to the elements within the documents that are part of the file that will be considered by the EDPB in making its decision[28].

26. Once the file has been declared complete, LSA and CSA(s) are in principle not able to submit any additional information concerning the subject matter of the dispute (unless requested by the Secretariat with a view of remedying an omission in accordance with Article 11(2) RoP[29]). Only in exceptional circumstances can the Board decide to consider further documents that it deems necessary. For example, the LSA cannot introduce new elements of fact supporting its decision not to follow one or more objections which were not previously communicated before the matter was referred to the EDPB[30]. Moreover, all information relevant to the assessment of the objections raised should already be exchanged between the LSA and CSA prior to the initiation of the Article 65(1)(a) procedure in an endeavour to reach consensus (as in doing so it may also help avoid the need for trigger the dispute resolution mechanism).

[21] Article 11(2) RoP provides that in exceptional circumstances, the EDPB can decide to consider further documents it deems necessary. As a result, the additional information may be requested by the Secretariat/Chair but the EDPB will have to decide if it will consider or not the additional info received.
[22] The competent authority must express its agreement with the translation provided (Article 11(2) RoP).
[23] Article 11(2) RoP.

[24] Article 11(2) RoP.
[25] Article 11(2) RoP.
[26] Such a time-frame should be decided on a case-by-case basis, taking into account the nature and volume of the documents requested. The Secretariat should consult with the LSA (or where applicable, CSA) to seek their views as to what constitutes an appropriate timeframe.
[27] See in particular Article 11(2) RoP: "[…] *together with confirmation and evidence of which documents submitted to the Board were provided to them when they were invited to exercise their right to be heard or a clear identification of the elements for which it is not the case.*"
[28] See Section 5 for additional information regarding the exercise of the right to be heard.
[29] See paragraph 20 above.
[30] Indeed, the wording of Article 11(2)d RoP confirms that when launching the procedure, the LSA should give an "indication" as to whether it does not follow the relevant and reasoned objection or is of the opinion that the objection is not relevant or reasoned (i.e. simply an indication as to whether it follows or not the objections). As a result, no new elements may be submitted going beyond those of which the CSAs were informed prior to the submission to the Board.

27. Once the file has been declared complete and the subject matter has been referred to the EDPB, the EDPB must issue a binding decision in relation to each objection raised, unless the CSA who raised a particular objection decides to withdraw it. As the withdrawal of the objection signifies the end of the dispute between the LSA and CSA, it is no longer necessary for the EDPB to resolve the matter[31]. Similarly, the LSA may be able to withdraw a referral to the EDPB on the basis of Article 60(4) GDPR in cases where it later decides that it would like to follow each of the objections raised. The withdrawal of either an objection or referral should occur only in very exceptional cases, however, as the obligation for LSA and CSAs to seek consensus under Article 60 GDPR requires that the dispute resolution mechanism will only be triggered in cases of persistent disagreement and where reaching consensus was not possible.

3.3 Establishment of deadline(s)

28. The default legal deadline for the EDPB to adopt a binding decision is one month after the Chair and the competent supervisory authority have decided that the file is complete[32]. The deadline may be extended by a further month on account of the complexity of the subject-matter[33]. If the EDPB has not been able to adopt a decision, upon expiry of such an extension, it shall do so within two weeks following the expiration of the extension[34].

3.3.1 Calculation

29. The calculation of the deadline for the adoption of the binding decision must be done on the basis of Regulation 1182/71[35]. According to Article 3(2)(c) of Regulation 1182/71,

> "*a period expressed in weeks, months or years shall start at the beginning of the first hour of the first day of the period, and shall end with the expiry of the last hour of whichever day in the last week, month or year is the same day of the week, or falls on the same date, as the day from which the period runs*".

The Court of Justice has confirmed that, for instance, if an event which is the point from which a period of a week starts to run happens on a Monday, the period will end on the following Monday, which will be the *dies ad quem* (deadline expiration date).[36] Likewise, if the time limit is expressed in months and the triggering event occurs on the 20th March, the period will end on the 20th April.

30. The start date ('*dies a quo*') in the application of Article 65(1)(a) GDPR consists of the day when the Chair and the competent supervisory authority have decided that the file is complete and the subject matter is referred to the EDPB by the Secretariat via the information and communication system mentioned in Article 17 of the EDPB Rules of Procedure.

[31] In cases where the withdrawal concerns the only objection which the LSA has decided not to follow or considered as not relevant and reasoned, the EDPB shall no longer be required to issue a binding decision in accordance with Article 65(1)(a) GDPR.
[32] Article 65(2) GDPR in conjunction with Article 11(4) RoP.
[33] Article 65(2) GDPR.
[34] Article 65(3) GDPR. See also paragraph 32.
[35] Regulation (EEC, Euratom) No 1182/71 of the Council of 3 June 1971 determining the rules applicable to periods, dates and time limits, O.J. 8.6.197, L 124/1. Article 40 RoP confirms that "*In order to calculate the periods and time limits expressed in the GDPR and in these Rules of Procedure, Regulation 1182/71 of the Council of 3 June 1971 determining the rules applicable to periods, dates and time limits shall apply*".
[36] See the Judgment in *Maatschap Toeters, MC Verberk v. Productschap Vee en Vlees*, C-171/03, ECLI:EU:C:2004:714, paragraph 33.

31. Since the GDPR does not express periods in working days, the time limits concerned include public holidays, Sundays and Saturdays[37]. However, when the last day of a period is a public holiday, Sunday or Saturday, the period shall end with the expiry of the last hour of the following working day[38], thus the deadline expiration date ('*dies ad quem*') shall be the following working day.

3.3.2 Decision to extend by one month

32. Article 65(2) GDPR allows the first one-month deadline to be extended by a further month, taking into account the complexity of the subject-matter. The extension needs to be decided by the Chair of the EDPB, either on its own initiative or at the request of at least one third of the members of the EDPB[39]. The extension decision must be taken prior to the expiration of the one month deadline.

3.3.3 Extension by two weeks

33. The binding decision must in principle be adopted by two-thirds majority at the latest two months after the file has been considered complete and the subject-matter has been referred to the EDPB. However, if the EDPB has not been able to adopt a decision within the extended timeframe because the required majority is not reached, the EDPB shall then adopt the decision within two weeks following the expiration of the second month by simple majority of its members[40].

34. During the two additional weeks, modifications can be made to the draft binding decision that was previously submitted for adoption by two-thirds majority if necessary to achieve the simple majority. In other words, the draft binding decision may be adapted and adjusted in case the two-thirds majority is not reached.

3.4 Preparation of the draft EDPB binding decision

35. According to Article 11(5) RoP, the binding decisions "*shall be prepared and drafted by the secretariat and, upon decision of the Chair, together with a rapporteur and expert subgroups members*"[41]. Therefore, the EDPB Secretariat should act as lead rapporteur and the Chair should decide on the involvement of an expert subgroup and of co-rapporteurs.

36. As soon as the LSA has submitted the matter to the EDPB for dispute resolution, the Secretariat should start the assessment of the completeness of the file. During this assessment, the Chair is invited to decide on the possible involvement of co-rapporteurs and will invite EDPB members to express an interest to become co-rapporteurs (unless the Chair decides not to involve co-rapporteurs for this case)[42]. In order to ensure fairness and impartiality, the (group of) co-rapporteur(s) should not include delegations from either the LSA or CSAs that submitted objections in relation to the draft decision[43].

[37] Article 3(3) of Regulation 1182/71.
[38] Article 3(4) of Regulation 1182/71.
[39] Article 11(4) RoP.
[40] See Article 65(3) GDPR. Regarding the calculation of the majority and voting rights of EDPB members see further Section 3.5 (Adoption of the EDPB binding decision).
[41] See also Article 75(6)(g) GDPR, which provides that the Secretariat shall be responsible in particular for the preparation, drafting and publication of decisions on the settlement of disputes between supervisory authorities.
[42] If the call for expression of interests to serve as co-rapporteur is made prior to the assessment that the file is complete, care should be taken not to disclose any elements of the file until after the assessment has been made and the subject matter has been referred to the EDPB.
[43] See also the Judgment in *Dr. August Wolff GmbH & Co. KG Arzneimittel*, Case C-680/16 P, 27 March 2019, ECLI:EU:C:2019:257, paragraphs 29-41.

37. Finally, it should be noted that the Chair may also decide to involve the members of one or more other expert subgroups, depending on the needs of the case.

38. As indicated earlier, Article 11(2) RoP states that the EDPB shall take into account *only* the documents which were provided by the LSA and the other CSA(s) once the matter is referred to the EDPB. This means that the LSA or CSA(s) cannot during the drafting stage introduce new elements of fact supporting their respective positions.

39. In accordance with Article 76(1) GDPR, discussions of the Board and of expert subgroups shall be confidential when they concern the consistency mechanism[44]. Moreover, an obligation of professional secrecy is also imposed on the staff of all EEA national supervisory authorities[45], the EDPS and the EDPB Secretariat[46]. This means that the duty of confidentiality and professional secrecy, which is of paramount importance, shall be respected by the EDPB and its members also in relation to Article 65(1)(a) dispute resolution cases. This concerns both the discussions and the documents exchanged.

3.5 Adoption of the EDPB binding decision

40. All majorities referred to by the GDPR (or by the RoP) refer to the total number of members of the EDPB entitled to vote, regardless of whether they are present or not[47].

41. While not having the right to vote, EFTA EEA supervisory authorities (i.e. Iceland, Liechtenstein and Norway) shall have the right to express their positions on all items discussed and/or voted[48].

42. In accordance with Article 68(6) GDPR, the EDPS shall have voting rights only on decisions which concern principles and rules applicable to the Union institutions, bodies, offices and agencies which correspond in substance to those of the GDPR. Where that is the case, the EDPS is entitled to vote on the decision as a whole.

43. Every EDPB member entitled to vote who is not represented at a plenary meeting can delegate its voting rights to another member of the Board entitled to vote and attending the plenary meeting[49].

44. The majority required for the adoption of a binding decision under Article 65(1)(a) GDPR is two-thirds of the EDPB members entitled to vote[50]. Where the EDPB has been unable to adopt a decision by two-thirds majority, the EDPB shall adopt its decision within the following two weeks by simple majority. Where the members of the Board are split, the decision shall by adopted by the vote of the Chair[51].

3.6 Notification to the supervisory authorities concerned

[44] Article 33 RoP.
[45] Article 54 (2) GDPR.
[46] Article 56 of Regulation (EU) 2018/1725.
[47] Article 22(3) RoP.
[48] See the Decision of the EEA joint Committee No 154/2018 of 6 July 2018 amending Annex XI (Electronic communication, audiovisual services and information society) and Protocol 37 (containing the list provided for in Article 101) to the EEA Agreement [2018/1022], See also Recital (7) and Article 4(1) RoP.
[49] The Chair and the secretariat shall be notified of any delegation of voting rights. Article 22(5)5 RoP.
[50] Article 65(2) GDPR in conjunction with Article 22(3) RoP.
[51] Article 65(3) GDPR.

45. Once the EDPB has adopted its binding decision, the Chair of the EDPB shall notify the decision to all the supervisory authorities concerned without undue delay[52]. Therefore, all the CSAs in the case need to be notified of the draft decision.

46. The notification will be performed by the Secretariat on behalf of the Chair via the information and communication system mentioned in Article 17 RoP.

3.7 Final Decision of the supervisory authority(ies)

47. Within one month after the notification of the EDPB decision to the supervisory authorities, the LSA and/or CSA (as the case may be[53]) must adopt a final decision[54]. Each final decision must be adopted "on the basis of" the decision of the EDPB. Moreover, the final decision(s) must refer to the decision by the EDPB and must specify that this decision will be published on the EDPB website. The final decision(s) of the LSA and/or CSA shall also "attach" the decision of the EDPB[55].

3.7.1 "On the basis of"

48. The requirement of adopting a final decision "on the basis of" the EDPB decision reflects the fact that the EDPB's decision is legally binding upon the LSA (and/or eventually the CSA(s) in case of need to adopt a final decision toward the data subjects[56]) as addressee(s) of the decision[57].

49. The aim of the binding decision is to resolve conflicting views among the LSA(s) and CSA(s) on the merits of the case, in particular whether there is an infringement of the GDPR, in order to ensure the correct and consistent application of the GDPR in individual cases[58].

50. The final decision must be adopted on the basis of the EDPB's decision and must, therefore, give full effect to the binding direction(s) as set out in the EDPB's decision. For example, if the EDPB has determined that there has indeed been an infringement of the GDPR, the LSA or CSA may not determine otherwise. In the same vein, if the EDPB has determined that envisaged action in relation to the controller or processor does not comply with the GDPR, the LSA or CSA must adapt their course of action accordingly[59].

3.7.2 Decision(s) by LSA and/or CSA

51. The final decision of the LSA and, as the case may be, the CSA with whom the complaint has been lodged, shall be adopted under the terms of Article 60(7), (8) and (9) GDPR[60].

52. The point of departure is that the LSA will be required to adopt and notify its final decision to the main establishment or single establishment of the controller or processor and inform the other supervisory authorities concerned as well as the EDPB of its final decision (including a summary of the relevant

[52] Article 65(5) GDPR.
[53] In case of partial or complete dismissal of a complaint, see Article 60(8) and (9) GDPR.
[54] Article 65(6) GDPR.
[55] The requirement that the final decision « attach » the EDPB decision does not mean that the EDPB decision must be annexed to the final decision within a single document (it is sufficient that the EDPB decision is communicated to the controller or processor together with the final decision).
[56] See Article 60(8) and (9) GDPR.
[57] Recital (136) and (143) GDPR.
[58] Recital (136) and Article 65(1)(a) GDPR.
[59] See Section 4 (Competence of the EDPB), in particular section 4.2 (Matters subject of the relevant and reasoned objection).
[60] Article 65(6) GDPR.

facts and grounds)[61]. One important derogation to this requirement concerns the situation where a complaint has been dismissed or rejected.

53. In cases where a complaint has been dismissed or rejected, the supervisory authority with which the complaint was lodged shall adopt the decision and notify it to the complainant and shall inform the controller thereof[62].

54. In case of need to take a decision to only partially dismiss a complaint, the LSA shall adopt the decision for the part concerning actions in relation to the controller or the processor, shall notify it to the main establishment or single establishment of the controller or processor on the territory of its Member State and shall inform the complainant thereof, while the supervisory authority of the complainant shall adopt the decision for the part concerning dismissal or rejection of that complaint, and shall notify it to that complainant and shall inform the controller or processor thereof[63].

55. Each natural or legal person has the right to an effective judicial remedy before the competent national court against a decision of a supervisory authority which produces legal effects concerning that person, in line with Article 78 GDPR[64].

3.7.3 Notification of the EDPB

56. The LSA or, as the case may be, the CSA with which the complaint has been lodged, is required to inform the EDPB of the date when its final decision is notified respectively to the controller or the processor and to the data subject[65].

3.8 Publication of the EDPB binding decision

57. In accordance with Article 65(5) GDPR, the publication of the EDPB binding decision on the website of the Board shall occur "without undue delay" after the LSA has notified the final national decision to the controller/processor and/or the CSA has notified the data subject (in case of a dismissal of a complaint). Whenever possible, "without undue delay" should be interpreted as suggesting that the publication of the EDPB binding decision should happen on the same day where the final national decision is notified to the controller/processor/complainant.

58. In order to allow the EDPB to publish its binding decision "without undue delay" after the notification of the final national decision, Article 65(6) GDPR requires the competent supervisory authority to inform the Board of the date when its final decision is notified respectively to the controller or processor and to the data subject. To avoid undue delays, each competent supervisory authority should inform the Secretariat of the date on which notification of the national decision is expected to take place, preferably at least one day in advance.

59. Article 339 TFEU requires the members and staff of the EU institutions not to disclose information of the kind covered by the obligation of professional secrecy, in particular information about undertakings, their business relations or their cost components[66]. As a consequence, some portions of the EDPB binding decision may need to be redacted in order to avoid disclosure of information covered by professional secrecy. The Secretariat will evaluate the need to redact such elements on the basis of EU law and the case law of the CJEU[67].

60. The EDPB will also publish the final national decision(s) in its register[68], taking into consideration possible restrictions under national law of the competent supervisory authority concerning the publication of its decisions. Where such restrictions apply, the SAs should inform the Secretariat of any such restrictions.

4 COMPETENCE OF THE EDPB

61. The aim of the consistency mechanism, including Article 65(1)(a) GDPR, is to contribute to the **consistent application** of the GDPR throughout the Union. Recital (136) clearly indicates that the competence of the EDPB to issue a binding decision in case of conflicting views among LSA and CSAs in the context of the cooperation mechanism relates to the **merits of the case**, in particular whether there is an infringement of the GDPR[69].

62. According to Article 65(1)(a) GDPR, the EDPB binding decision shall concern **all the matters which are the subject of the relevant and reasoned objection**. Therefore, the EDPB will assess **only** issues included in the objections that have been raised in relation to the draft or revised draft decision of the LSA. The EDPB will not reassess the whole case nor will it address issues that might be raised in the course of the Article 65 procedure but were not the subject of the reasoned and relevant objections submitted prior to the submission of the dispute to the EDPB.

63. The dispute between the LSA and the CSA(s) may concern either the fact that the LSA does not follow one or more relevant and reasoned objections or that the LSA is of the opinion that one or more objections is not relevant or reasoned. The EDPB will assess, in relation to each objection raised, whether the objection meets the requirements of Article 4(24) GDPR and, if so, address the merits of the objection in the binding decision.

4.1 Assessment of whether the objections are relevant and reasoned

[61] Article 60(7) GDPR.
[62] Article 60(8) GDPR.
[63] Article 60(8) GDPR.
[64] See also Recital (143) GDPR. See further Section 8 (Judicial remedies).
[65] Article 65(6) GDPR.
[66] An obligation of professional secrecy is also imposed on the staff of the EU institutions by the Staff Regulations and on the staff of the EDPS, including the EDPB Secretariat, also by Article 56 of Regulation (EU) 2018/1725. An obligation of professional secrecy is also imposed by Article 54 (2) GDPR on the members and staff of each supervisory authority.
[67] See, for instance, Judgments in *Bank Austria Creditanstalt*, T-198/03, 30 May 2006, ECLI:EU:T:2006:136; in *Evonik Degussa*, T-341/12, 28 January 2015, ECLI:EU:T:2015:51; in *Akzo Nobel NV*, T-345/12, 28 January 2015, ECLI:EU:T:2015:50; in *MasterCard, Inc.*, T-516/11, 9 September 2014, EU:T:2014:759; in *Stichting Greenpeace Nederland*, T-545/11 RENV, 21 November 2018, ECLI:EU:T:2018:817; in *Amicus Therapeutics UK Ltd*, T-33/17, 25 September 2018, ECLI:EU:T:2018:595; in *Pergan Hilfsstoffe für industrielle Prozesse GmbH*, Case T-474/04 , 12 October 2007, [2007] ECR II-4225.
[68] Article 70(1)(y) GDPR requires the EDPB to maintain a publicly accessible electronic register of decisions taken by supervisory authorities and courts on issues handled in the consistency mechanism. See https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-decisions.
[69] Recital (136) stipulates that "*[…] The Board should also be empowered to adopt legally binding decisions where there are disputes between supervisory authorities. For that purpose, it should issue, in principle by a two-thirds majority of its members, legally binding decisions in clearly specified cases where there are conflicting views among supervisory authorities, in particular in the cooperation mechanism between the lead supervisory authority and supervisory authorities concerned on the merits of the case, in particular whether there is an infringement of this Regulation.*"

64. In its Guidelines on relevant and reasoned objections, the EDPB has clarified the conditions that must be met in order for an objection to be considered "relevant and reasoned" within the meaning of Article 4(24) GDPR[70].

65. When a LSA refers a dispute to the EDPB for resolution in accordance with Article 60(4) and 63 GDPR, the EDPB must first assess whether the objection(s) raised in fact meet the conditions of being relevant and reasoned[71].

66. The EDPB recalls that in order for an objection to be considered as "relevant", there must be a direct connection between the objection and the substance of the draft decision at issue. More specifically, the objection needs to concern either whether there is an infringement of the GDPR or whether the envisaged action in relation to the controller or processor complies with the GDPR[72].

67. In order for an objection to be "reasoned", it should be coherent, clear, precise and detailed in explaining the reasons for the objection. It should set forth, clearly and precisely, the essential elements on which the CSA based its assessment, and the link between the envisaged consequences of the draft decision (if it was to be issued as it is) and the significance of the anticipated risks for data subjects' fundamental rights and freedoms and, where applicable, for the free flow of personal data within the Union[73].

68. When assessing whether the objections in fact meet the conditions of being relevant and reasoned, the assessment carried out by the EDPB will be both **substantial and formal**. In other words, the EDPB will take into account the specific wording used by the CSA within each of the objections raised and whether each element of Article 4(24) GDPR is explicitly mentioned in relation to each specific objection; thus requiring an explicit reference to the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects[74].

69. In its binding decision, the EDPB will not take any position on the merits of any substantial issues raised by objections that do not meet the conditions of Article 4(24) GDPR. If an objection does not meet the conditions of Article 4(24) GDPR, the binding decision of the EDPB remains without any prejudice to any assessments the EDPB may be called upon to make in other cases, including with the same parties, taking into account the contents of the relevant draft decision and the objections raised by the CSAs.

4.2 Matters subject of the relevant and reasoned objection

70. In its Guidelines on relevant and reasoned objections, the EDPB also clarified the possible subject matter (substance) of a relevant and reasoned objection[75]. Those Guidelines describe a number of examples of objections that may meet the requirements of Article 4(24) GDPR. These examples relate to possible disagreements between the LSA and CSA on the following matters:

1. the existence of a given infringement of the GDPR;
2. the existence of additional or alternative infringements of the GDPR;
3. gaps in the draft decision justifying the need for further investigation;
4. insufficient factual information or reasoning;
5. procedural aspects; and
6. the specific action envisaged by the draft decision.

4.2.1 Existence of a given infringement of the GDPR

71. A first example of a possible relevant and reasoned objection involves the disagreement between the LSA and CSA as to whether or not a given provision of the GDPR has been infringed[76]. Such a disagreement may arise where the draft decision adopted by the LSA either:

- explicitly confirms the existence of an infringement of a specific article of the GDPR, but the CSA considers that this article of the GDPR has not been infringed[77];
- explicitly confirms that a particular article of the GDPR has not been infringed, whereas the CSA considers that the article in question has been infringed.

72. In accordance with Article 65(1)(a) GDPR, the EDPB shall take a binding decision concerning all the matters which are the subject of the relevant and reasoned objections, "*in particular whether there is an infringement of the GDPR*". The EDPB must make a binding decision which shall whenever possible, taking into account the elements of the file and the right to be heard, provide a final conclusion on the application of the GDPR in relation to the case at hand. In other words, the EDPB shall assess the merits of the arguments raised by the CSA in the objection against those of the LSA and make a final determination as to whether or not the given infringement of the GDPR took place or not. The EDPB will instruct the LSA to alter a finding of an infringement or to include one whenever necessary. In such cases, the LSA will then be obliged to implement the change in its final decision, taking into account the binding decision of the EDPB in relation to the objection raised.

4.2.2 Additional or alternative infringements of the GDPR

73. A second example of a possible relevant and reasoned objection involves disagreement between the LSA and CSA as to the conclusions to be drawn from the findings of the investigation. For instance, the objection may state that the findings amount to the infringement of a provision of the GDPR other than (and/or in addition to) those already analysed by the draft decision[78].

74. As previously indicated, the EDPB must make a binding decision which shall whenever possible, taking into account the elements of the file and the respondent's right to be heard, provide a final conclusion on the application of the GDPR in relation to the case at hand. This can potentially include a determination of the existence of additional (or alternative) infringements, provided that the file contains sufficient factual elements to substantiate the alleged infringement and the persons who

[70] RRO GLS, paragraphs 12-21.
[71] As clarified earlier, the LSA shall submit the matter to the EDPB either if it does not follow the relevant and reasoned objection *or* if it is of the opinion that the objection is not relevant or reasoned. See section 3.1 above.
[72] RRO GLS, paragraph 12. An objection raised fulfils the criterion of being "relevant" when, if followed, it would entail a change leading to a different conclusion as to whether there is an infringement of the GDPR or as to whether the envisaged action in relation to the controller or processor, as proposed by the LSA, complies with the GDPR. RRO GLS, paragraph 13.
[73] RRO GLS, paragraph 19. See also RRO GLS, paragraph 16. ("*In order for the objection to be "reasoned", it needs to include clarifications and arguments as to why an amendment of the decision is proposed (i.e. the legal / factual mistakes of the LSA's draft decision). It also needs to demonstrate how the change would lead to a different conclusion as to whether there is an infringement of the GDPR or whether the envisaged action in relation to the controller or processor complies with the GDPR.*").
[74] See also RRO GLS, paragraphs 7 and 37.
[75] RRO GLS, paragraphs 22-48.
[76] RRO GLS, paragraphs 24-25.
[77] The RRO GLS include the following example : The CSA argues that LSA did not take into consideration the fact that the household exemption is not applicable to some of the processing operations conducted by a controller and involving the use of CCTV, hence that there is no infringement of the GDPR.
[78] RRO GLS, paragraph 26.

would be adversely affected have been or can be heard in relation to the objections alleging the existence of an additional or alternative infringement[79].

Example 3:

The draft decision of a LSA states that the controller failed to comply with the duty to inform pursuant to Article 14 GDPR (information to be provided where personal data have not been obtained from the data subject). The draft decision states that the controller should have provided the information in paragraphs 14(1) and 14(2)(a) and (e) GDPR and finds no other infringements of Article 14. One of the CSAs considers that the controller should have provided all the information referred to in Article 14(2)(b) and (f) GDPR, as the default position is that all such information set out in that subarticle should be provided to the data subject unless one or more categories of the information does not exist or is not applicable.[80] Provided the objection raised by the CSA meets the requirements of Article 4(24), and taking into account the elements of the file and the right to be heard, the EDPB will decide whether or not the controller additionally infringed Article 14(2)(b) and (f) GDPR, in addition to Article 14(1) and Art. 14(2)(a) and (e) GDPR.

75. If the EDPB determines, following a relevant and reasoned objection to this effect, that additional and/or alternative provisions of the GDPR have been infringed, the LSA will be obliged to reflect this in its final decision, taking into account the binding decision of the EDPB in relation to the objection raised.

76. It may be possible, in exceptional cases, that the file submitted to the EDPB does not contain sufficient factual elements to allow the EDPB to make a final conclusion regarding the existence of the infringement identified by the relevant and reasoned objection. In most cases, however, the information exchanged during the cooperation procedure should be sufficient to enable the CSA to substantiate its objection in such a way that the EDPB shall be able make a final determination whether or not there has been an infringement of the GDPR[81]. Furthermore, when the LSA submits the matter to the Secretariat to obtain a binding decision on the basis of Article 65(1)(a) GDPR, the Secretariat may also request the LSA and/or CSA to provide additional information that is necessary to ensure the file is complete[82].

4.2.3 Gaps in the draft decision justifying the need for further investigation by the LSA

77. A third example of a possible relevant and reasoned objection involves disagreement between the LSA and CSA as to whether the draft decision has sufficiently investigated the relevant infringements of the GDPR[83].

Example 4:

The LSA, upon receiving a complaint, considers that not all of the allegations of infringements contained in the complaint merit investigation. In its draft decision, the LSA only addresses those aspects of the complaint which it decided to investigate without any statement regarding the other alleged infringements of the GDPR. The CSA considers that the LSA in its investigation unjustifiably failed to address a number of alleged infringements raised by the complainant and submits a relevant and reasoned objection based on the failure of the LSA to properly handle the complaint to safeguard the rights of the data subject.

78. Article 57(1)(f) GDPR imposes a duty upon supervisory authorities to handle each and every complaint submitted to them and to investigate the subject matter of the complaint "to the extent appropriate". The term "to the extent appropriate" provides the competent supervisory authority with a margin of discretion as regards the extent or depth of the investigation needed. However, this discretionary power must be exercised with all due diligence[84] and in accordance with the relevant provisions of the GDPR implying mutual cooperation.

79. If the EDPB, on the basis of a relevant and reasoned objection, determines that the LSA has unjustifiably failed to investigate or in any other way address some of the issues raised by the complaint, the EDPB can issue a binding decision specifying the need for LSA to handle the matter further and to investigate – to the extent appropriate – the remaining subject matter of the complaint. To the extent that the draft decision allows it, the LSA should in principle first seek to finalise its draft decision as regards those matters that do not require further investigation within the deadline specified by Article 65(6).

80. For those matters requiring further investigation, it may be necessary for the LSA to open a new case file. In case a new case file is opened to address the remaining issues, the LSA is required to comply with all cooperation provisions under the GDPR. This may lead to submitting a new draft decision in accordance with A60(3) GDPR which addresses the outstanding alleged infringement. In situations where it is not possible for the LSA to follow this course of action (e.g., when there is inextricable link between the matter requiring further investigation and the other parts of the LSA's draft decision that are to be finalised), it may be necessary for the LSA to first investigate the matter further and prepare an updated draft decision.

81. In any event, the LSA shall be required to further address the matter and keep the members of the EDPB informed of the steps taken. Moreover, the CSAs can seek to use the cooperation and consistency mechanisms provided for in the GDPR in case the LSA does not fulfil its obligations flowing from the Article 65 decision (i.e addressing the remaining issues to be resolved) [85].

4.2.4 Insufficient factual information or reasoning

82. A fourth example of a possible relevant and reasoned objection involves disagreement between the LSA and CSA as to whether sufficient factual elements and/or reasoning have been included in the draft decision[86]. For instance, a CSA might consider that the conclusion by the LSA included the draft decision is not adequately supported by the assessment carried out and the evidence presented[87]. In such a case the EDPB shall also be competent to issue a binding decision, provided the objection raised

[79] See section 5 regarding the right to be heard.
[80] See also Article 29 Working Party Guidelines on transparency under Regulation 2016/679, 29 November 2017, WP260 rev.01, 11 April 2018, paragraph 46.
[81] Where appropriate, the CSA and LSA can make use of Article 61 and 62 GDPR with a view of obtaining the necessary information prior to the issuance of the draft decision.
[82] See section 3.2 above.
[83] RRO GLS, paragraph 27.
[84] Judgment in *Schrems*, C-362/14, 6 October 2015, ECLI:EU:C:2015:650, paragraph 63.
[85] The EDPB recalls the possibility for CSAs make use, where appropriate, of the ability to request mutual assistance pursuant to Article 61 GDPR (which also allow CSAs, in case the LSA fails to comply, to adopt a provisional measure in accordance with Article 66) or requests for an opinion pursuant to Article 64(2) GDPR (which is explicitly deemed by the legislator as particularly appropriate where a SA does not comply with its obligations for mutual assistance under Article 61 GDPR). The latter procedure may, eventually, produce a binding decision of the EDPB in accordance with Article 65(1)(c) GDPR. See also Advocate General Bobek, Opinion in *Facebook Ireland Limited*, C-645/19, ECLI:EU:C:2021:5, paragraphs 115-121. Additionally, the EDPB may also, in its binding decision under Article 65(1)(a) GDPR, invite the CSA to request the LSA to further investigate via an Article 61 Mutual Assistance request.
[86] RRO GLS, paragraph 29.
[87] *Ibid*.

meets the whole threshold of Article 4(24) GDPR, including a link between the allegedly insufficient analysis and the existence of an infringement or the envisaged action[88].

83. In a situation where the draft decision of the LSA contains insufficient factual elements or reasoning, there are essentially two possible scenarios.

84. In the first scenario, the file on the basis of which the EDPB shall make its decision already contains sufficient information that would allow to address the lack of sufficient factual elements or reasoning in the draft decision. In such cases, the EDPB shall, within the scope of the relevant and reasoned objection, determine to what extent the LSA should amend its draft decision in order to remedy the insufficiency of reasoning, by making reference to the relevant elements included in the file.

> **Example 5:**
>
> The draft decision of the LSA establishes an infringement of the GDPR based on findings of fact supported by documentary evidence which were provided in the file to the EDPB. A number of CSAs submit relevant and reasoned objections outlining that the link between the documentary evidence and the finding of infringement is not sufficiently reasoned in the draft decision. The EDPB decision finds that the objection(s) are relevant and reasoned and indicates the correct legal interpretation and reasoning that the LSA should incorporate in its final decision.

85. In the second scenario, the file on the basis of which the EDPB shall make its decision does not contain sufficient factual elements to address the insufficiency of factual elements or reasoning.

> **Example 6:**
>
> The draft decision of the LSA finds that there is no infringement of Article 6(1)(a) GDPR and that the processing in question is lawful on the basis of the data subject's consent. However, neither the draft decision nor any other document in the file provides any further materials or analysis as to whether the conditions of Article 7 GDPR have been met. The draft decision simply states that the processing has been lawfully based on consent, without providing further reasoning or evidence. A CSA raises an objection against this lack of reasoning, arguing that the absence of this analysis gives rise to uncertainty surrounding the finding of no infringement in this case.

If the EDPB determines that the file on the basis of which the EDPB shall make its decision does not contain sufficient factual elements that would allow to remedy the insufficiency of reasoning, the EDPB can issue a binding decision specifying the need for LSA to investigate or address the matter further with a view of obtaining sufficient factual information, in line with what is specified in paragraphs 79-81 above.

4.2.5 Procedural aspects

86. A fifth example of a possible relevant and reasoned objection involves a disagreement between the LSA and CSA as to whether the procedural requirements imposed by the GDPR have been properly respected and this affects the conclusion reached in the draft decision[89].

87. The EDPB recalls that the aim of the dispute resolution mechanism of Article 65(1)(a) GDPR is to resolve conflicting views on the merits of the case[90]. It is not intended to resolve possible disputes regarding procedural requirements or duties of cooperation[91].

[88] RRO GLS, paragraph 29.
[89] RRO GLS, paragraph 30.
[90] See above at paragraph 61.
[91] In this regard, the EDPB recalls Articles 61, 64(2), 65(1)(c) and 66 of the GDPR.

88. An objection involving a disagreement concerning procedural requirements will only be considered relevant and reasoned if the objection also puts forward arguments clarifying the different conclusion that the LSA should have reached in its draft decision. In its decision, the EDPB will resolve the dispute surrounding the conclusions reached in the draft decision.

89. If the procedural deficiencies leave the EDPB unable to resolve the dispute surrounding the conclusions reached by the draft decision (e.g. due to a lack of sufficient factual elements), the EDPB will recall the importance of the duty of cooperation and issue a binding decision specifying the need for LSA to investigate or address the matter further, in line with what is specified in paragraphs 79-81 above and ensuring full compliance with the procedural requirements in the GDPR which were not met.

4.2.6 Action envisaged

90. A sixth example of a possible relevant and reasoned objection involves disagreement between the LSA and CSA as to whether the envisaged action in relation to the controller or processor complies with the GDPR[92].

91. The EDPB recalls that Recital (150) GDPR states that the consistency mechanism may also be used to promote a consistent application of administrative fines. As a result, if the assessment of the EDPB within this context identifies shortcomings in the reasoning leading to the imposition of the fine at stake, the LSA will be instructed to re-assess the fine and remedy the identified shortcomings[93].

92. Fines are by no means the only action a supervisory authority can envisage. A relevant and reasoned objection may therefore also relate to other envisaged actions, taking into account the range of powers listed in Article 58(2) GDPR. Each envisaged measure should be appropriate, necessary and proportionate in view of ensuring compliance with this Regulation, taking into account the circumstances of each individual case[94]. In this context, it should be recalled that the decision to reject or dismiss a complaint, in whole or in part, also constitutes an envisaged action capable of being subject of a relevant and reasoned objection.

93. If the EDPB, on the basis of a relevant and reasoned objection, determines that the envisaged action included in the draft decision does not comply with the GDPR, it shall instruct the LSA to re-assess the envisaged action and change the draft decision in accordance with the binding decision of the EDPB.

[92] See also RRO GLS, paragraphs 32 et seq.
[93] RRO GLS, paragraph 34.
[94] Recital (129) GDPR.

5 THE RIGHT TO BE HEARD

5.1 Applicability

94. The right to be heard before an administration takes a measure that would adversely affect a person is enshrined in Article 41 CFEU and has long been recognised as a general principle of EU law[95]. The right to be heard is also included in Article 16 of the European Code of Good Administrative Behaviour and reflected in Article 11 RoP.

95. Article 41 CFEU is addressed not to the Member States but solely to the institutions, bodies, offices and agencies of the European Union[96]. Nevertheless, the right to be heard has also been recognised as "*inherent in respect for the rights of the defence, which is* ***a general principle of EU law***"[97] and therefore also applies when Member States adopt decisions which come within the scope of EU law[98].

96. The right to be heard applies to administrative proceedings of which the outcome is likely to affect the (legal or natural) person's interests. It also applies in situations where the administration of EU law is divided or shared between EU and the Member States (so-called "composite procedures"[99]). Article 41(2)(a) CFEU is framed in terms of individual measures that would adversely affect the person, with no specific requirement that the contested measure should be initiated against that person[100].

97. Article 65(2) GDPR provides that the EDPB's decision "*shall be […] addressed to the lead supervisory authority and all the supervisory authorities concerned and binding on them*". Article 65(2) GDPR reflects the fact that the binding decision of the EDPB aims to resolve a dispute that has emerged among two or more national supervisory authorities. In accordance with the procedure under Article 60 GDPR, LSA will have shared its legal analysis in the draft decision and in relation the objections raised during the cooperation procedure. The CSA(s) likewise will have shared its (their) objection(s) in relation to the draft decision, including any materials to substantiate their objection. In addition, both the LSA and CSAs can share their views in the course of the preparation and adoption of the EDPB decision[101].

98. Article 65(2) GDPR also confirms that the EDPB decision does not address directly any party other than the LSA and CSAs. Nevertheless, the decision adopted by the EDPB at European level shall be binding on the LSA or, as the case may be, the CSA with which the complaint has been lodged and is therefore decisive for the outcome of the procedure at national level. It therefore also may affect the interests of persons who were part of the procedure that gave rise to the draft decision.

99. As a result, any of these persons which would be adversely affected by the decision, in particular the controller(s) and/or processor(s) who are addressed by the draft decision of the LSA, as well as any other person which would be adversely affected by the decision, must be afforded the right to be heard in relation to the subject matter which is brought before the EDPB pursuant to Articles 60(4), 63 and 65(1)(a) GDPR.

5.2 Purpose

100. The right to be heard is described by the Court as guaranteeing "*every person the opportunity to make known his views effectively during an administrative procedure and before the adoption of any decision liable to affect his interests adversely*"[102]. As clarified by the CJEU, the purpose of the rule, that the addressee of an adverse decision must be placed in a position to submit his observations before that decision is taken, is to put the competent authority in a position effectively to take all relevant information into account. In order to ensure that the person concerned is in fact protected, the purpose of that rule is, inter alia, to enable that person to correct an error or submit such information relating to his or her personal circumstances as will argue in favour of the adoption or non-adoption of the decision, or in favour of it having a specific content[103].

101. The right to respond is also part of the right to be heard since an "*administrative procedure requires that the person concerned should be able […] to put his own case and properly make his views known on the relevant circumstances and, where necessary, on the documents taken into account by the Community institutions*"[104]. Except in cases where legislation expressly provides for the possibility of an oral hearing, such as in the competition proceedings, the right to be heard does not necessarily require an oral hearing[105].

5.3 Timing

5.3.1 At national level and prior to referral to the EDPB

102. Before the EDPB is given the task of issuing a binding decision, every supervisory authority is under and obligation to respect the right to be heard in the context of its national procedure, as a general principle of EU law[106]. Indeed, every supervisory authority needs to "*respect the right of every person to be heard before any individual measure which would affect him or her adversely is taken*"[107]. The right to be heard applies regardless of whether the case is cross-border in nature or not.

103. Even in the absence of specific provisions under national law, the LSA should, in advance of triggering Article 65(1)(a) GDPR, ensure that procedure conducted at national level takes into account the requirements of the right to be heard as a general principle of EU law.

---

[95] See e.g. Judgment in *France v. Commission*, C-301/87, 14 February 1980, paragraph 29.
[96] See e.g. Judgment in *Cicala*, C-482/10, 21 December 2011, ECLI:EU:C:2011:868, paragraph 28.
[97] See e.g. Judgment in *Mukarubega*, C-166/13, 5 November 2014, ECLI:EU:C:2014:2336, paragraph 45.
[98] *Ibid*., paragraph 46. See also Judgments in *Glencore Agriculture Hungary Kft.*, C-189/18, 16 October 2019, ECLI:EU:C:2019:861, paragraph 39 ("*[….] The authorities of the Member States are subject to that obligation when they take decisions which come within the scope of EU law, even though the EU law applicable does not expressly provide for such a procedural requirement")* and in *Teodor Ispas*, Case C-298/16, 9 November 2017, ECLI:EU:C:2017:843, paragraph 26. See also the Opinion of Advocate General Bobek in *Teodor Ispas*, Case C-298/16, 7 September 2017, ECLI:EU:C:2017:650, paragraphs 35-69.
[99] Regarding composite administrative procedures, see e.g. the Opinion of Advocate General Compos Sánchez-Bordana in *Silvio Berlusconi*, Case C-219/17, 27 June 2018, ECLI:EU:C:2018:502, paragraphs 57-79. See also F. Brito Bastos, "Beyond Executive Federalism. The Judicial Crafting of the Law of Composite Administrative Decision-Making", Thesis submitted for assessment with a view to obtaining the degree of Doctor of Laws of the European University Institute, Florence, 13 June 2018, in particular at p. 120-163.
[100] P. Craig, "Article 41 - Right to Good Administration", in *EU Charter of Fundamental Rights : A Commentary*, edited by Steve Peers, et al., Bloomsbury Publishing, 2014, p. 1079.
[101] However, according to the RoP, in exceptional circumstances, the EDPB can decide to consider further documents (Article 11(2) in fine RoP).

[102] See e.g. Judgments in *M.M.*, C-277/11, 22 November 2012, EU:C:2012:744, paragraph 87; *Mukarubega*, paragraph 46; *Glencore Agriculture Hungary*, paragraph 39 and the case law cited therein.
[103] Judgment in *Glencore*, paragraph 41 and 52.
[104] See e.g. the Judgment in *Technische Universität Munchen*, C-269/90, 21 November 1991, paragraph 25.
[105] See Article 12 of Regulation 773/2004 (O.J 27 April 2004, L 123, p. 18). See also the Opinion of Advocate General Wahl in *SKW Stahl-Metallurgie GmbH and Holding AG v European Commission*, C-154/14, 3 September 2015, ECLI:EU:C:2015:543, paragraphs 45-47.
[106] See paragraphs 95 above.
[107] Recital (129) GDPR.

5.3.2 During the assessment of completeness of the file

104. When the LSA submits the matter to the Secretariat with a view of obtaining a binding decision of the EDPB under Article 65(1)(a) GDPR, the Secretariat should assess which persons would possibly be adversely affected by the EDPB decision in the sense of Article 41 of the Charter. It should also assess whether each of those persons was offered the opportunity to exercise its right to be heard.

105. It is not sufficient that the LSA has heard the persons who might be adversely affected in the course of the national procedure prior to the adoption of its draft decision within the meaning of Article 60(3) GDPR. Before the EDPB will be in a position to resolve the dispute, the right to be heard must also be afforded in relation to any objections raised in relation to the draft decision, in particular where the LSA chooses not to follow the objection (or considers it as not being relevant reasoned).

106. When submitting the matter to the Secretariat, the LSA is expected to demonstrate how the right to be heard has been afforded to persons benefitting from this right in the course of the national procedure leading to the draft decision. As regards the documents shared when submitting the matter to the Secretariat, the LSA should specifically mention whether or not these documents (or the relevant contents thereof[108]) were subject to the right to be heard and with regard to which persons[109]. Replies or summaries of the hearing(s) should be provided as well.

107. The accommodation of the right to be heard is an essential element of the procedure, in the absence of which the subject matter of the dispute cannot be settled by the EDPB. As a result, the gathering and verification of the relevant information is carried out in the context of the check on the completeness of the file, before the subject matter is referred to the EDPB. Only after all the relevant verifications have been made by the Secretariat, the Chair shall be in the position to declare the file complete[110].

108. If there are relevant documents or information that have not been subject to the right to be heard, the Chair may instruct the Secretariat to ask the supervisory authorities (LSA / CSA) to take the necessary actions to enable any party that could be affected to be heard. If necessary, the Chair may instruct the Secretariat to take measures to directly ensure the right to be heard at the EDPB level. In both instances, the persons who would be adversely affected shall be invited to exercise the right to be heard on the relevant documents or information within a specific timeframe, taking into account the complexity of the subject matter (as well as possible needs for translation).

[108] For purposes of the procedure under Article 65(1)(a) GDPR, the scope of which is limited resolving disputes concerning the objections raised, the right to be heard does not need to extend to elements beyond the subject matter of the dispute.
[109] See Article 11(2)(f) RoP, which specifies that the LSA when submitting the matter to the Secretariat should include, *inter alia*, "*"In accordance with Article 41 of the European Charter on Fundamental Rights, the written observations the LSA collected from the persons that might be adversely affected by the Board's decision, together with confirmation and evidence of which documents submitted to the Board were provided to them when they were invited to exercise their right to be heard or a clear identification of the elements for which it is not the case*".
[110] See also section 3.2 above.

6 ACCESS TO THE FILE

109. The right to good administration includes the right of every person to have access to the file, while respecting the legitimate interests of confidentiality and of professional and business secrecy[111].

110. Access to the documents and information that form the basis of an administrative decision is closely connected with the right to be heard[112]. In accordance with that principle, 'the addressees of decisions which significantly affect their interests must be placed in a position in which they can effectively make known their views as regards the *information on which the authorities intend to base their decision*'[113].

111. The right of access to the file of the EDPB as part of the right to good administration is distinct from the general right of access to documents held by the European institutions, bodies, offices and agencies pursuant to Regulation (EC) No 1049/2001[114], Article 15(3) TFEU or Article 42 of the Charter[115]. The right of access to the file and the right of access to documents are subject to different criteria and exceptions and pursue different purposes.

112. The right of access to the file extends to the documents shared with the EDPB to resolve the dispute in accordance with Article 65(1)(a) procedure, save where they involve business secrets of other undertakings, confidential information, as assessed by the EDPB on a case by case basis.

113. The right of access to the file shall not extend to confidential information and internal documents of the EDPB or the SAs (e.g. email correspondence or preparatory documents). In particular, the right of access shall not extend to exchanges between the EDPB and its members once the procedure has been launched[116].

[111] Article 41(2)b CFEU. The SA acting on behalf of the EDPB cannot make a general reference to confidentiality to justify a total refusal to disclose documents in its file to persons adversely affected, nor can it give blank pages on the ground that they contained business secrets without providing a more comprehensible non-confidential version, or a summary of the documents.
[112] Opinion of Advocate General Bobek in *Teodor Ispas*, Case C-298/16, 7 September 2017, ECLI:EU:C:2017:650, paragraphs 117 and following.
[113] Opinion of Advocate General Bobek in *Teodor Ispas*, Case C-298/16, 7 September 2017, ECLI:EU:C:2017:650, paragraphs 117 and following. See in the same vein also Opinion of Advocate General Bobek in *Glencore Agriculture Hungary Kft.*, C-189/18, 16 October 2019, ECLI:EU:C:2019:861, paragraph 51
[114] Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents (OJ L 145, 31.5.2001, p. 43). Article 2(1) of Regulation (EC) No 1049/2001 sets out that any citizen of the EU, and any natural or legal person residing or having its registered office in a Member State, has a right of access to documents of the EU institutions, subject to the principles, conditions and limits defined in that Regulation.
[115] Article 32 RoP.
[116] See also Article 33 RoP.

7 THE DUTY TO GIVE REASONS

114. The right to good administration contained in Article 41 CFEU also includes the obligation of the administration to give reasons for its decisions[117].

115. The duty to give reasons entails informing the addressee of the decision of the **factual and legal grounds** on which it is based, thereby enabling the person to decide whether to seek judicial review and facilitate the exercise of that review by the courts[118].

116. The EDPB must articulate, in a clear and unequivocal fashion the reasoning underlying in its decision in such a way as to enable the persons affected to ascertain the reasons for its decision. While the EDPB does not need to state *all* legal and factual reasons leading to its decision, it must explain those which were of *decisive* importance[119]. In the same vein, the EDPB is also not obliged to adopt an explicit position on all the arguments raised. It is sufficient for the decision to set out, in a clear and unambiguous manner, the principal issues of law and of fact upon which it is based and which are necessary in order that the reasoning which has led the EDPB to its decision may be understood. What ultimately matters is that the statement of reasons by the EDPB enables all persons affected by the decision to ascertain whether the relevant provisions have been applied correctly.

117. The EDPB must in its statement of reasons set out all the relevant grounds and motives for the adoption of its decision – including those that originate from the national level. This means that insofar as the facts set out in the draft decision or related documents are decisive for the decision of the EDPB, then the EDPB should include them in its statement of reasons[120].

118. In relation to objections where the EDPB simply agrees with the reasons contained in the draft decision by the LSA or the decision of the LSA not to follow the relevant and reasoned objection (or to consider them not relevant or reasoned), the EDPB may fulfil its duty to state reasons by simply referring back to the position of the LSA, provided the affected persons were informed of those positions of the LSA and given the opportunity to be heard in relating to those positions[121].

119. In light of the aforementioned considerations, the binding decision adopted by the EDPB on the basis of Article 65(1)(a) GDPR should in principle include a summary of dispute as well as an assessment of whether the conditions for adopting a binding decision are met. For each objection raised, the EDPB will then in principle[122]:

[117] Article 41(2)c CFEU.
[118] See e.g., Judgment in *Métropole Télévision SA*, T-206/99, 21 March 2011, paragraph 44. See also P. Craig, "Article 41 - Right to Good Administration", in *EU Charter of Fundamental Rights: A Commentary*, edited by Steve Peers, et al., Bloomsbury Publishing, 2014, p. 1085.
[119] See e.g. Judgments of the General Court in *L'Air liquide*, Cases T-185/06, 16 June 2011, EU:T:2011:275, paragraph 64; in *Ryanair Ltd*, T-123/09, 28 March 2012, EU:T:2012:164, paragraph 178-179; and in *FIH Holding A/S*, T-386/14, 15 September 2016, EU:T:2016:474, paragraph 94.
[120] Based on F. Brito Bastos, "Beyond Executive Federalism. The Judicial Crafting of the Law of Composite Administrative Decision-Making", Thesis submitted for assessment with a view to obtaining the degree of Doctor of Laws of the European University Institute, Florence, 13 June 2018, p. 176 and following.
[121] *Ibid*.
[122] The draft binding decision of the EDPB should in principle synthesize the main elements of facts preceding the dispute, together with a summary of the main arguments put forth, unless the specific wording used is essential for a proper discussion/understanding of the issue at stake.

- summarise main elements of the draft decision which are related to the subject matter of the objection;
- summarise the main elements of the objection raised;
- summarise the position of the LSA or CSA in relation to the objection raised; and
- summarise the position of the persons who may be adversely affected in relation to the objection.

Once the relevant elements have been set out, the EDPB will assess, in relation to each objection raised, whether the EDPB meets requirements of Article (24) GDPR and, if so, address the merits of the objection in the binding decision[123].

120. The operative parts of the decision should be clearly identified as such and included at the end of the decision, rendering explicit to what extent the competent authority is required/not required to amend its draft decision before finalisation.

8 JUDICIAL REMEDIES

121. Article 47 of the Charter guarantees the right to an effective remedy and to a fair trial. This is linked to the need to ensure the compatibility of the acts of the EU institutions with the European Union legal order, which is a task generally entrusted to the Court of Justice and to the courts of the European Union.

122. Good administrative behaviour entails informing persons affected by the measure of the available appeal mechanism[124]. The EDPB decision will refer to the possibilities open to appeal it (i.e. to seek annulment), whereas the competent supervisory authority will refer to the appeal mechanisms available at national level. The competent supervisory authority may in its final decision also choose make reference to the possibilities to seek annulment of the decision of the EDPB on the basis of which the final decision was adopted, as clarified by Recital (143) GDPR (in addition to providing information regarding possible appeal mechanisms at national level in relation to its final decision).

[123] It should be noted that the EDPB does not take any position on the merit of any substantial issues raised by objections deemed not to meet the requirements stipulated by Article 4(24) GDPR. Where that is the case, the decision of the EDPB is without any prejudice to any assessments the EDPB may be called upon to make in other cases, including with the same parties, taking into account the contents of the relevant draft decision and the objections raised by the CSAs.
[124] See also Commission 'Code of Good administrative behaviour', Point 3, third indent: 'Where Community law so provides, measures notified to an interested party should clearly state that an appeal is possible and describe how to submit it, (the name and office address of the person or department with whom the appeal must be lodged and the deadline for lodging it).Where appropriate, decisions should refer to the possibility of starting judicial proceedings and/or of lodging a complaint with the European Ombudsman in accordance with Article 230 or 195 of the Treaty establishing the European Community.' European Ombudsman 'Code of Good administrative behaviour', Article 19 - indication of the possibilities of appeal: 'A decision of the Institution which may adversely affect the rights or interests of a private person shall contain an indication of the appeal possibilities available for challenging the decision. It shall in particular indicate the nature of the remedies, the bodies before which they can be exercised, as well as the time limits for exercising them. Decisions shall in particular refer to the possibility of judicial proceedings and complaints to the European Ombudsman under the conditions specified in, respectively, Articles [263] and Articles [228 TFEU].'

123. While Recital (143) refers to the possibility of persons directly and individually concerned by a decision of the EDPB bringing an action for annulment before the CJEU, the position on standing will ultimately be assessed by the CJEU in light of the conditions provided for in Article 263 TFEU.

124. An action for annulment before the Court of Justice does not suspend the effects of the decision of the EDPB[125]. The competent SAs will therefore still have to comply with the decision of the EDPB adopted on the basis of Article 65(1)(a) GDPR, notwithstanding the appeal. This is without prejudice to the right to effective judicial remedy by the controller or processor at national level in accordance with Article 78 GDPR.

8.1 Supervisory authorities

125. Article 65(2) GDPR makes clear that decisions adopted by the EDPB on the basis of Article 65(1)(a) GDPR are binding upon the lead supervisory authority and all the concerned supervisory authorities. National SAs must adopt their final decision on the basis of the EDPB decision. Article 65(2) also makes clear the decision is an act "addressed to" the LSA and the CSAs - it does not directly address any third parties[126].

126. According to Recital (143) GDPR, as addressees of the decisions of the Board, the concerned supervisory authorities which wish to challenge them have to bring action within two months of being notified of them, in accordance with Article 263 TFEU. This means, *inter alia*, that the supervisory authorities acting before the Court of Justice against a binding decision of the EDPB would need to do so relying on one of the listed grounds for annulment contained in Article 263 TFEU.

127. Although only the LSA and some CSAs (pursuant to Article 60(8) and (9) GDPR) shall adopt their national decision on the basis of the EDPB binding decision, the decision is addressed to all the CSAs involved in the cross-border case. Article 65(2) GDPR mentions all the CSAs as addressees of the decision and the final national decision is the product of a co-decision making process which is strongly affected by the decision of the EDPB. As a consequence, all the supervisory authorities that are concerned in a given cross-border case (see Article 4(22) GDPR) are "addressed" by the decision and therefore entitled to bring action for annulment of the EDPB decision.

128. Although the supervisory authorities concerned, as Members of the EDPB, gain knowledge of the content of the EDPB binding decision in the occasion of its adoption pursuant to Article 65(2) GDPR, the time limitation for them to bring action will start when the decision is notified to them by the EDPB Secretariat, acting on behalf of the Chair[127] and using the internal information and communication system[128].

[125] Article 278 TFEU (ex Article 242 TEC): "*Actions brought before the Court of Justice of the European Union shall not have suspensory effect. The Court may, however, if it considers that circumstances so require, order that application of the contested act be suspended.*"
[126] See also paragraph 98 above.
[127] See, e.g. Judgment of the General Court in *Access Info Europe v Council*, T-233/09, ECLI:EU:T:2011:105, paragraph 28 ("*Where the addressee has been notified, it is the date of notification which is to be taken into consideration for the purposes of calculating the time allowed […] for bringing proceedings, not the date on which cognisance was taken, which comes into play only as an alternative in cases where there is no notification*").
[128] See Article 17 EDPB RoP.

8.2 Controller, processor, complainant, or other entity

129. Entities other than the addressees may be entitled to act before the Court of Justice for the annulment of the EDPB binding decision if the decision is of direct and individual concern to them[129].

130. Recital (143) explicitly mentions that controllers, processors, or complainants may be directly and individually concerned by an EDPB binding decision. These requirements are, however, interpreted restrictively by the Court of Justice and therefore a case-by-case analysis is necessary[130].

131. The action for annulment by a controller, processor or complainant, needs to be brought within two months of the publication of the EDPB binding decision on the website of the Board[131]. As indicated earlier, the publication of the EDPB's decision on its website occurs without delay after the final national decision is notified to the controller, processor and/or data subject[132].

132. Since the national decision needs to attach the EDPB decision, the person who receives notification of the national decision will at the same time receive the Article 65(1)(a) decision. However, this does not amount to "notification" of the EDPB decision in the sense of the Treaties as interpreted by the CJEU[133]. Additionally, according to Article 263 TFEU and the CJEU case law, the criterion of the day on which a measure comes to the knowledge of the applicant is a subsidiary one, i.e. it is only relevant where the act is neither published nor notified to the applicant[134]. Consequently, the two-month period starts when the decision is published on the website of the Board.

133. Without prejudice to this right under Article 263 TFEU, each natural or legal person also has an effective judicial remedy before the competent national court against those final decisions taken by supervisory authorities, which produces legal effects concerning that person[135]. This right has to be exercised in accordance to the applicable national legislation. Article 78(4) GDPR specifies that where proceedings are brought against a decision of a supervisory authority which was preceded by an opinion or decision of the Board in the consistency mechanism, the supervisory authority shall forward that opinion or decision to the court.

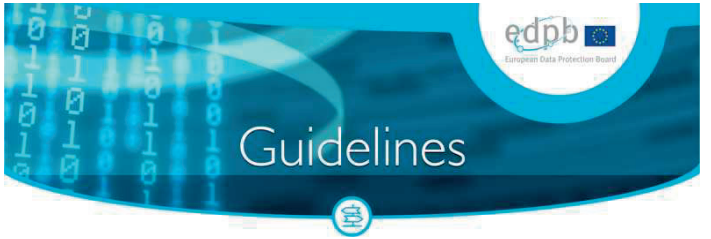
134. Where a decision of a supervisory authority implementing an Article 65 GDPR decision of the EDPB is challenged before a national court and the validity of the decision of the EDPB is at issue, the national court does not have the power to declare the EDPB's Article 65 GDPR decision invalid. Where it

[129] Recital (143) GDPR.
[130] See also the Opinion of Advocate General Bobek in *Facebook Ireland Limited*, C-645/19, ECLI:EU:C:2021:5, footnote 52.
[131] Recital 143 GDPR.
[132] Article 65 (5) GDPR.
[133] According to the CJEU case law, "*notification is the operation by which the author of a decision of individual relevance communicates the latter to the addressees and thus puts them in a position to take cognisance of it*" (Judgment of the Court of First Instance in *Olsen v Commission*, T-17/02, ECLI:EU:T:2005:218, paragraph 74).
[134] Judgment of the Court of First Instance in *Olsen v Commission*, T-17/02, ECLI:EU:T:2005:218, paragraphs 73 and 81 (specifying that "*the criterion of the day on which a measure came to the knowledge of an applicant, as the starting point of the period prescribed for instituting proceedings, is subsidiary to the criteria of publication or notification of the measure*", and therefore where there is publication "*it is of little importance whether the applicant had sufficient knowledge of the contested decision [earlier]*" since that "*issue is not relevant for determining the starting point of the period for bringing an action because it is not appropriate to apply […] the criterion of the day on which a measure came to the knowledge of an applicant, which is provided for in the alternative*" in Article 263 TFEU).
[135] Recital (143) GDPR. This includes the exercise of investigative, corrective, and authorisation powers, or the dismissal or rejection of complaints, but not including non-legally binding measures.

considers the decision invalid, it must refer the question of validity to the Court of Justice in accordance with Article 267 TFEU[136].

135. However, a national court may not refer a question on the validity of a decision of the EDPB when the requesting natural or legal person was under the legal conditions to bring an action for annulment of that decision before the CJEU (in particular if it was directly and individually concerned), but had not done so within the two-month period laid down in Article 263 TFEU. Therefore, when the directly and individually concerned persons decide to not bring an action for annulment of the EDPB binding decision, this will prevent them from challenging the validity of the EDPB binding decision in front of national courts.

[136] Recital (143) GDPR.



Guidelines 02/2021 on virtual voice assistants

Version 2.0

Adopted on 7 July 2021

Version history

Version 2.0	7 July 2021	Adoption of the Guidelines after public consultation
Version 1.0	9 March 2021	Adoption of the Guidelines for publication consultation

EXECUTIVE SUMMARY

A virtual voice assistant (VVA) is a service that understands voice commands and executes them or mediates with other IT systems if needed. VVAs are currently available on most smartphones and tablets, traditional computers, and, in the latest years, even standalone devices like smart speakers.

VVAs act as interface between users and their computing devices and online services such as search engines or online shops. Due to their role, VVAs have access to a huge amount of personal data including all users' commands (e.g. browsing or search history) and answers (e.g. appointments in the agenda).

The vast majority of VVA services have been designed by few VVA designers. However, VVAs can work jointly with applications programmed by third parties (VVA application developers) to provide more sophisticated commands.

To run properly, a VVA needs a terminal device provided with microphones and speakers. The device stores voice and other data that current VVAs transfer to remote VVA servers.

Data controllers providing VVA services and their processors have therefore to consider both the GDPR[1] and the e-Privacy Directive[2].

These guidelines identify some of the most relevant compliance challenges and provide recommendations to relevant stakeholders on how to address them.

Data controllers providing VVA services through screenless terminal devices must still inform users according to the GDPR when setting up the VVA or installing, or using a VVA app for the first time. Consequently, we recommend to VVA providers/designers and developers to develop voice-based interfaces to facilitate the mandatory information.

Currently, all VVAs require at least one user to register in the service. Following the obligation of data protection by design and by default, VVA providers/designers and developers should consider the necessity of having a registered user for each of their functionalities.

The user account employed by many VVA designers bundle the VVA service with other services such as email or video streaming. The EDPB considers that data controllers should refrain from such practices as they involve the use of lengthy and complex privacy policies that would not comply with the GDPR's transparency principle.

The guidelines consider four of the most common purposes for which VVAs process personal data: executing requests, improving the VVA machine learning model, biometric identification and profiling for personalized content or advertising.

Insofar the VVA data is processed in order to execute the user's requests, i.e. as strictly necessary in order to provide a service requested by the user, data controllers are exempted from the requirement of prior consent under Article 5(3) e-Privacy Directive. Conversely, such consent as required by Article

[1] Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter "GDPR").
[2] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) as amended by Directive 2006/24/EC and Directive 2009/136/EC (hereinafter "e-Privacy Directive").

5(3) e-Privacy Directive would be necessary for the storing or gaining of access to information for any purpose other than executing users' request.

Some VVA services retain personal data until their users require their deletion. This is not in line with the storage limitation principle. VVAs should store data for no longer than is necessary for the purposes for which the personal data are processed.

If a data controller becomes aware (e.g. due to quality review processes) of the accidental collection of personal data, they should verify that there is a valid legal basis for each purpose of processing of such data. Otherwise, the accidentally collected data should be deleted.

VVAs may process data of multiple data subjects. VVA providers/designers should therefore implement access control mechanisms to ensure personal data confidentiality, integrity and availability. However, some traditional access control mechanisms such as passwords are not fit for the VVA context since they would have to by spoken aloud. The guidelines provide some considerations on this regard, including a section specific to the processing special categories of data for biometric identification.

VVA providers/designers should consider that when collecting user's voice, the recording might contain other individuals' voice or data such as background noise that is not necessary for the service. Whenever possible, VVA designers should therefore consider technologies filtering the unnecessary data and ensuring that only the user voice is recorded.

When evaluating the need for a Data Protection Impact Assessment (DPIA), the EDPB considers that it is very likely that VVA services fall into the categories and conditions identified as requiring a DPIA.

Data controllers providing VVA services should ensure users can exercise their data subject rights using easy-to-follow voice commands. VVA providers/designers, as well as app developers should at the end of the process inform users that their rights have been duly factored, by voice or by providing a writing notification to the user's mobile, account or any other mean chosen by the user.

Table of contents

EXECUTIVE SUMARY 2
1 GENERAL 7
2 TECHNOLOGY BACKGROUND 8
2.1 Basic characteristics of Virtual Voice Assistants 8
2.2 Actors in the VVA ecosystem 9
2.3 Step-by-step description 10
2.4 Wake-up expressions 11
2.5 Voice snippets and machine learning 11
3 ELEMENTS OF DATA PROTECTION 12
3.1 Legal framework 12
3.2 Identification of data processing and stakeholders 14
3.2.1 Processing of personal data 14
3.2.2 Processing by data controllers and processors 15
3.3 Transparency 17
3.4 Purpose limitation and legal basis 21
3.4.1 Execute users' requests 21
3.4.2 Improve the VVA by training the ML systems and manually reviewing of the voice and transcripts 22
3.4.3 User identification (using voice data) 23
3.4.4 User profiling for personalized content or advertising 23
3.5 Processing of children's data 25
3.6 Data retention 25
3.7 Security 27
3.8 Processing of special categories of data 29
3.8.1 General considerations when processing special categories of data 30
3.8.2 Specific considerations when processing biometric data 30
3.9 Data minimization 32
3.10 Accountability 32
3.11 Data protection by design and by default 33
4 Mechanisms to exercise Data Subject Rights 33
4.1 Right to access 34
4.2 Right to rectification 35
4.3 Right to erasure 35
4.4 Right to data portability 36

5 Annex: Automatic Speech Recognition, Speech Synthesis and Natural Language Processing 37
5.1 Automatic Speech Recognition (ASR) 38
5.2 Natural Language Processing (NLP) 38
5.3 Speech Synthesis 38

The European Data Protection Board

Having regard to Article 70 (1j) and (1e) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, (hereinafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018[3],

Having regard to Article 12 and Article 22 of its Rules of Procedure,

HAS ADOPTED THE FOLLOWING GUIDELINES

1 GENERAL

1. Recent technological advances have greatly increased the accuracy and popularity of virtual voice assistants (VVA). Among other devices, VVAs have been integrated in smartphones, connected vehicles, smart speakers and smart TVs. This integration has given the VVAs access to information of an intimate nature that could, if not properly managed, harm the individuals' rights to data protection and privacy. Consequently, VVAs and the devices integrating them have been under the scrutiny of different data protection authorities.
2. There are several advantages to using speech-based interactions such as: the naturalness of the interaction which does not involve specific learning from the users, the speed of execution of the command and the extension of the field of action which can allow faster access to information. However, relying on speech also brings in difficulties in interpreting the message correctly: variability of the audio signal between different speakers, acoustic environment, ambiguity of the language, etc.
3. In practice, the fluidity or simplification of tasks remains the primary motivation for equipping oneself with VVAs. This may involve, for example, placing/answering a call, setting a timer, etc., especially when the users have their hands unavailable. Home automation is the major application put forward by the designers of VVAs. By proposing to simplify the execution of tasks (turning on the light, adjusting the heating, lowering the shutters, etc.) and to centralize them through a single tool that can be easily activated remotely, they fit into the discourse as a domestic facilitator. In addition to personal or domestic use, voice commands can be of interest in professional environments where it is difficult to handle computer tools and use written commands (e.g. manufacturing work).
4. In theory, the main beneficiaries of the voice interface could be people with disabilities or dependency for whom the use of traditional interfaces is problematic. Virtual voice assistance can provide easier access to information and computer resources and thus promote inclusive

[3] References to "Member States" made throughout this document should be understood as references to "EEA Member States".

logics as the use of the voice makes it possible to overcome the difficulties associated with the written word, which can be found among certain classes of users.

5. Finally, health is also an area where there are many cases of use for conversational agents, vocal or not. For instance, during the Covid-19 pandemic, various callbots were deployed to offer a pre-diagnosis to calling users. In the long term some anticipate that the entire patient care process could be impacted by human/assistant interactions: not only for well-being and prevention, but also for treatment and support.

6. There are currently more than 3 billion smartphones and all of them have integrated VVAs, most of them switched on by default. Some of the most widespread operating systems in personal computers and laptops also integrate VVAs. The recent rise of smart speakers (147 million were sold in 2019[4]) is bringing VVAs to millions of homes and offices. However, current VVA designs do not offer by default authentication or access control mechanisms.

7. This document seeks to provide guidance as to the application of the GDPR in the context of the VVAs.

2 TECHNOLOGY BACKGROUND

2.1 Basic characteristics of Virtual Voice Assistants

8. A VVA can be defined as a software application that provides capabilities for oral dialogue with a user in natural language.

9. Natural language has a semantics specific to human language. Depending on the characteristics of the language and the diversity of the lexicon, the same instruction can be formulated in multiple ways, whereas some commands may seem similar but relate to two different objects. Inference mechanisms are then frequently used to resolve these ambiguities, for example, depending on what has been said previously, the time when the instruction was given, the place, the person's interests, etc.

10. A VVA can be broken down into modules allowing to perform different tasks: sound capture and restitution, automatic speech transcription (speech to text), automatic language processing, dialogue strategies, access to ontologies (data sets and structured concepts related to a given domain) and external knowledge sources, language generation, voice synthesis (text to speech), etc. Concretely, the assistant should allow interaction in order to perform actions (e.g. "turn on the radio", "turn off the light") or to access knowledge (e.g. "what will the weather be like tomorrow?", "is the 7:43 a.m. train running?"). It thus plays the role of intermediary and orchestrator who is supposed to facilitate the accomplishment of the user's tasks.

11. In practice, a VVA is not a smart speaker but a smart speaker can be equipped with a voice assistant. It is common to confuse both of them, however, the latter is only a material incarnation of the former. A VVA can be deployed in a smartphone, a smart speaker, a connected watch, a vehicle, a household appliance, etc.

[4] For example, see a press release of 1 August 2019 by the Hamburg Data Protection and Information authority: https://datenschutz-hamburg.de/pressemitteilungen/2019/08/2019-08-01-google-assistant

12. The organization of the underlying data processing may involve multiple information flow patterns. It is possible to isolate three main entities:

    The physical instance: the hardware element in which the assistant is embodied (smartphone, speaker, smart TV, etc.) and which carries microphones, speakers and network and computing capacities (more or less developed depending on the case).

    The software instance: the part implementing the human-machine interaction strictly speaking and which integrates the modules for automatic speech recognition, natural language processing, dialogue and speech synthesis. This can be operated directly within the physical equipment, but in many cases is performed remotely.

    The resources: external data such as content databases, ontologies or business applications that provide knowledge (e.g. "tell the time on the West Coast of the United States", "read my emails") or enable the requested action to be carried out in a concrete way (e.g. "increase the temperature by 1.5°C").

13. VVAs allow the installation of third party components or apps that expand their core functionalities. Each VVA name the components differently but all involve the exchange of users' personal data between the VVA designer and the app developer.

14. Although most VVAs do not share the voice snippet with the app developers, these actors still process personal data. Moreover, depending on the nature of the functionality provided, the app developer receives intentions and slots which could include sensitive information like health data.

2.2 Actors in the VVA ecosystem

15. A VVA may involve a great number of actors and intermediaries throughout the execution chain. In practice, up to five different actors can be identified. Depending on business models and technological choices, some actors may however take on several combinations of roles, for example, designer and integrator or designer and application developer:

    a. **The VVA provider (or designer):** responsible for the development of the VVA, designs and defines its possibilities and default functionalities: activation modalities, choice of architecture, data access, record management, hardware specifications, etc.

    b. **The VVA application developer:** as for mobile applications, creates applications extending the VVA's default functionalities. To do this, it is necessary to respect the development constraints imposed by the designer.

    c. **The integrator:** manufacturer of connected objects, who wishes to equip them with a VVA. It should respect the requirements defined by the designer.

    d. **The owner:** in charge of physical spaces receiving people (accommodation places, professional environments, rental vehicles, etc.) he/she wishes to provide a VVA to his/her audience (possibly with dedicated applications).

    e. **The user:** final link in the VVA value chain, who can use it on various devices (speaker, TV, smartphone, watch, etc.) depending on how and where the VVA has been deployed and set up.

2.3 Step-by-step description

16. In order for a VVA to carry out an action or to access information, a succession of tasks is carried out:

    1) Deployed within a piece of equipment (smartphone, loudspeaker, vehicle), the VVA is on standby. To be precise, it is constantly listening. However, until a specific wake-up expression has been detected no audio is transmitted out of the device receiving the voice and no other operation than wake-up expression detection is performed. For this purpose a buffer of a few seconds is used (see following section for more details).

    2) The user says the wake-up expression and the VVA locally compares the audio with the wake-up expression. If they match, the VVA opens a listening channel and the audio content is immediately transmitted.

    3) In many cases, if the processing of the command is done remotely, a second check of the keyword pronunciation is done on the server side to limit unwanted activations.

    4) The user states his request that is transmitted on the fly to the VVA provider. The sequence of speech spoken is then automatically transcribed (speech to text).

    5) Using natural language processing (NLP) technologies, the command is interpreted. The intentions of the message are extracted and information variables (slots) are identified. A dialogue manager is then used to specify the interaction scenario to be implemented with the user by providing the appropriate response scheme.

    6) If the command involves a functionality provided by a third party app (skill, action, shortcut, etc.), the VVA provider sends to the app developer the intentions and information variables (slots) of the message.

    7) A response adapted to the user's request is identified – at least supposedly, the answer "I don't have the answer to your question" being an adapted response in the case the VVA was not able to correctly interpret the request. If necessary, remote resources are used: publicly accessible knowledge databases (online encyclopaedia, etc.) or by authentication (bank account, music application, customer account for online purchase, etc.) and the information variables (slots) are filled with the recovered knowledge.

    8) An answer phrase is created and/or an action is identified (lowering the blinds, raising the temperature, playing a piece of music, answering a question, etc.). The sentence is synthesized (text to speech) and/or the action to be performed is sent to the equipment executed.

    9) The VVA returns to standby.

    Please note that while currently most voice related processing is performed in remote servers, some VVA providers are developing systems that could perform part of this processing locally[5].

[5] This has been reported, for example, here: https://www.amazon.science/blog/alexas-new-speech-recognition-abilities-showcased-at-interspeech

2.4 Wake-up expressions

17. In order to be used, a VVA should be "awake". This means that the assistant switches to an active listening mode in order to receive orders and commands from its user. While this wake-up can also sometimes be achieved by a physical action (e.g. by pressing a button, pressing the smart speaker, etc.), almost all VVAs on the market are based on the detection of a wake-up expression or word to switch to active listening mode (also known as activation word or wake-up word / hot word).

18. To do this, the assistant relies on the use of the microphone and slight computational capabilities to detect whether the keyword has been spoken. This analysis, which takes place continuously from the moment the VVA is on, is carried out exclusively locally. Only when the keyword has been recognised are the audio recordings processed for interpretation and execution of the command, which in many cases means sending them to remote servers via the Internet. Keyword detection is based on machine learning techniques. The major challenge in using such methods is that the detection is probabilistic. Thus, for each word or expression pronounced, the system provides a confidence score as to whether the keyword has actually been pronounced. If this score turns out to be higher than a predefined threshold value, this is considered to be the case. Such a system is therefore not free of errors: in some cases activation may not be detected even though the keyword has been said (false rejection) and in other cases activation may be detected even though the user has not said the keyword (false acceptance).

19. In practice, an acceptable compromise should be found between these two types of errors to define the threshold value. However, since the consequence of a false detection of the keyword might be the sending of audio recordings, unexpected and unwanted transmissions of data are likely to occur. Very often, VVA providers implementing remote processing use a two-pass mechanism for this detection: a first pass embedded locally at the equipment level and a second one performed on remote servers where the next data processing are taking place. In this case, developers tend to set up a relatively low threshold in order to enhance the user experience and ensure that when the user says the keyword, it is almost always recognized - even if this means "over-detecting" it - and then implement a second detection pass on the server side, which is more restrictive.

2.5 Voice snippets and machine learning

20. VVAs rely on machine learning methods to perform a wide range of tasks (keyword detection, automatic speech recognition, natural language processing, speech synthesis, etc.) and thus necessitate large datasets to be collected, selected, labelled, etc.

21. The over- or under-representations of certain statistical characteristics can influence the development of machine learning-based tasks and subsequently reflect it in its calculations, and thus in its way of functioning. Thus, just as much as its quantity, the quality of the data plays a major role in the finesse and accuracy of the learning process.

22. In order to increase the quality of the VVA and improve the machine learning methods deployed, VVA designers might wish to have access to data relating to the use of the device in real conditions – i.e. voice snippets – in order to work on its improvement.

23. Whether it is to qualify the learning database or to correct errors made when the algorithm is deployed, learning and training of artificial intelligence systems necessarily require human intervention. This part of the work, known as digital labor, raises questions about both working

conditions and safety. In this context, news media have also reported data transfers between VVA designers and subcontractors allegedly without the necessary privacy protection guarantees.

3 ELEMENTS OF DATA PROTECTION

3.1 Legal framework

24. The relevant EU legal framework for VVAs is in the first instance the GDPR, as processing of personal data belongs to the core function of the VVAs. In addition to the GDPR, the e-Privacy Directive[6] sets a specific standard for all actors who wish to store or access information stored in the terminal equipment of a subscriber or user in the EEA.

25. In accordance with the definition of "*terminal equipment*"[7], smartphones, smart TVs and similar IoT devices are examples for terminal equipment. Even if VVAs in themselves are a software services, they always operate through a physical device such as a smart speaker or a smart TV. **VVAs use electronic communications networks to access these physical devices that constitute "terminal equipment" in the sense of the e-Privacy Directive. Consequently, the provisions of Article 5 (3) e-Privacy Directive apply whenever VVA stores or accesses information in the physical device linked to it**.[8]

26. Any processing operations of personal data following the aforementioned processing operations, including processing personal data obtained by accessing information in the terminal equipment, must also have a legal basis under Article 6 GDPR in order to be lawful.[9]

27. Since the controller, when seeking consent for storing or gaining of access to information pursuant to Article 5(3) e-Privacy Directive, will have to inform the data subject about all the purposes of the processing (meaning the "subsequent processing") – including any processing following the aforementioned operations – consent under Article 6 GDPR will generally be the most adequate legal basis to cover the subsequent processing of the personal data. Hence, consent will likely constitute the legal basis both for the storing and gaining of access to information already stored and the processing of personal data following the aforementioned processing operations. Indeed, when assessing compliance with Article 6 GDPR, one should take into account that the processing as a whole involves specific activities for which the EU legislature has sought to provide additional protection.[10] Moreover, controllers must take into account the impact on data subjects' rights when identifying the appropriate lawful basis in order to respect the principle of fairness.[11] The bottom line is that Article 6 GDPR cannot be relied upon by controllers in order to lower the additional protection provided by Article 5(3) e-Privacy directive.

28. As shown in section 2.3 (steps 2 and 3), current VVAs require access to the voice data stored by the VVA device.[12] Therefore, Article 5(3) e-Privacy Directive applies. The applicability of Article 5 (3) e-Privacy Directive means that the storing of information as well as the accessing to information already stored in a VVA requires, as a rule, end-user's prior consent[13] but allows for two exceptions: first, carrying out or facilitating the transmission of a communication over an electronic communications network, or, second, as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user.

29. The second exception ("strictly necessary in order to provide an information society service explicitly requested by the subscriber or user") would allow a VVA service provider to process users' data to execute users' requests (see par. 72 in section 3.4.1) without the consent foreseen in Article 5(3) e-Privacy Directive. Conversely, such **consent as required by Article 5(3) ePrivacy Directive would be necessary for** the storing or gaining of access to information for **any purpose other than executing users' request** (e.g. user profiling). Data controllers would need to attribute consent to specific users. Consequently, data controllers should only process non-registered users data to execute their requests.

30. VVAs can accidentally capture audio of individuals who did not intend to use a VVA service. First, to a certain extent and depending on the VVAs, the wake-up expression can be changed. Individuals who are not aware of this change could accidentally use the updated wake-up expression. Second, VVAs can detect the wake-up expression by mistake or by error. It is highly unlikely that either of the exceptions foreseen in Article 5(3) e-Privacy Directive are applicable in the event of an accidental activation. Furthermore, consent as defined in the GDPR must be the "*unambiguous indication of the data subject's wishes*". Thus, it is highly unlikely that an accidental activation could be interpreted as a valid consent. If data controllers become aware (e.g. through automated or human review) that the VVA service has accidentally processed personal data, they should verify that there is a valid legal basis for each purpose of processing of such data. Otherwise, the accidentally collected data should be deleted.

31. Moreover, it should be noted that the personal data processed by VVAs may be highly sensitive in nature. It may carry personal data both in its content (meaning of the spoken text) and its meta-information (sex or age of the speaker etc.). The EDPB recalls that voice data is inherently biometric personal data.[14] As a result, when such data is processed for the purpose of uniquely identifying a natural person or is inherently or determined to be special category personal data, the processing must have a valid legal basis in Article 6 and be accompanied by a derogation from Article 9 GDPR (see section 3.7 below).

[6] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) as amended by Directive 2006/24/EC and Directive 2009/136/EC (hereinafter "e-Privacy Directive").

[7] Article 1 of Commission Directive 2008/63/EC of 20 June 2008 on competition in the markets in telecommunications terminal equipment, defines "*terminal equipment*" as (a) an "*equipment directly or indirectly connected to the interface of a public telecommunications network to send, process or receive information; in either case (direct or indirect), the connection may be made by wire, optical fibre or electromagnetically; a connection is indirect if equipment is placed between the terminal and the interface of the network; (b) satellite earth station equipment*";

[8] See EDPB Guidelines 1/2020 paragraph 12 for similar reasoning regarding connected vehicles (hereinafter "EDPB Guidelines 1/2020"). See also EDPB, Opinion 5/2019 on the interplay between the e-Privacy Directive and the GDPR, in particular regarding to competence, tasks and powers of data protection authorities.

[9] Ibid, paragraph 41.

[10] Opinion 5/2019, paragraph 41.

[11] EDPB Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0, 8 October 2019, paragraph 1.

[12] It is possible that future VVA devices will adopt the edge computing paradigm and be capable of providing some service locally. In such event, it will be necessary to reassess the applicability of the e-Privacy Directive.

[13] See also EDPB Guidelines 1/2020, paragraph 14.

[14] Article 4(14) GDPR defines biometric data as 'personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data'

3.2 Identification of data processing and stakeholders

32. Considering the multiple possibilities of assistance that a VVA can provide in so many different environments of a data subject's daily life,[15] it is worth noting that careful consideration should be taken with the processing of personal data, which can also be impacted by different stakeholders.

3.2.1 Processing of personal data

33. From a personal data protection perspective, several constants can be observed irrespective of the VVA type (i.e. type of device, functionalities, services or combination of them) that can be used by a data subject. Such constants relate to the plurality of personal data, data subjects and data processing at stake.

Plurality of personal data types

34. The definition of personal data under Article 4(1) GDPR includes a wide variety of different data and applies in a technologically neutral context to any information that relates "*to an identified or identifiable natural person*".[16] Any interaction of a data subject with a VVA can fall under the scope of this definition. Once the interaction takes place, diverse range of personal data may be processed throughout the operation of the VVA as described in section 2.4.

35. From the initial request to the related answer, action or follow-up (e.g. setting up a weekly alert), the first personal data input will therefore generate subsequent personal data. This includes primary data (e.g. account data, voice recordings, requests history), observed data (e.g. device data that relates to a data subject, activity logs, online activities), as well as inferred or derived data (e.g. user profiling). VVAs use speech to mediate between users and all the connected services (e.g. a search engine, an online shop or a music streaming service) but unlike other intermediaries, VVAs may have full access to the requests' content and consequently provide the VVA designer with a wide variety of personal data depending on the purposes of the processing.

36. The plurality of personal data processed when using a VVA, also refers to a plurality of personal data categories for which attention should be paid (see below section 3.7). The EDPB recalls that when special categories of data[17] are processed, Article 9 GDPR requires the controller to identify a valid exemption from the prohibition to processing in Article 9(1) and a valid legal basis under Article 6(1), using an appropriate means identified under Article 9(2). Explicit consent may be one of the appropriate derogations where consent is the legal basis relied on under Article 6(1). Article 9 also notes (in detail) that the Member States may introduce further conditions to processing of biometric or other special categories data.

[15] For example: at home, in a vehicle, in the street, at work or in any other private, public or professional spaces or a combination of these spaces.
[16] Article 4(1) GDPR also specifies that "*an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*".
[17] Article 9(1) GDPR defines special categories of personal as "*personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.*"

Plurality of data subjects

37. When using a VVA, personal data are processed from the first interaction with the VVA. For some data subjects this refers to the purchase of a VVA and/or the configuration of a user account (i.e. registered users). For other data subjects it refers to the first time they knowingly interact with the VVA of another data subject who purchased and/or configured this VVA (i.e. non-registered users). Besides these two categories of data subjects, there is a third one: accidental users who, registered or not, unknowingly make requests to the VVA (e.g. saying the correct wake-up expression without knowing the VVA is active, or saying other words that are mistakenly identified by the VVA as the wake-up expression).

38. The term plurality of data subjects also refers to multiple users for one VVA (e.g. device shared between registered and non-registered users, between colleagues, in a family, at school) and different types of users based on their condition (e.g. an adult, a child, an elder or a disable person). While a VVA can offer easier interaction with a digital tool and many benefits for some categories of data subjects, it is important to take into consideration the specificities of each category of data subjects and the context of use of the VVA.

Plurality of data processing

39. The technologies used to provide a VVA also have an impact on the amount of the processed data and the types of processing. The more a VVA provides services or features and is connected to other devices or services managed by other parties, the more the amount of personal data being processed and repurposing processing increases. This results in a plurality of processing carried out by automated means as described in section 2. Besides automated means, some processing may also involve human means. This is the case for example, when the implemented technology involves human intervention, such as the review of transcription of voices into texts, or the provision of annotations on personal data that can be used to insert new models in a machine-learning technology. This is also the case when humans analyse personal data (e.g. metadata) in order to improve the service provided by a VVA.

3.2.2 Processing by data controllers and processors

40. Data subjects should be in a position to understand and identify the roles at stake and should be able to contact or act with each stakeholder as required under the GDPR. The distribution of roles should not be to the detriment of the data subjects, even though scenarios can be complicated or evolving. In order to assess their roles, stakeholders are referred to the EDPB Guidelines 7/2020 on the concepts of controller and processor in the GDPR.[18]

41. As indicated in paragraph 15, the main stakeholders can be identified under the role of a provider or designer, an application developer, an integrator, an owner, or a combination of them. Different scenarios are possible, depending on who is doing what in the stakeholders' business relationship, on the user's request, the personal data, the data processing activities and their purposes. They should clearly decide and inform data subjects on the conditions under which each of them will act and comply with the resulting roles of controllers, joint-controllers or processors as provided for by the GDPR.[19] Each of them may take on one or

[18] EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, V2.0, adopted on 7 July 2021 (hereinafter "Guidelines 7/2020").
[19] GDPR, Articles 12-14, Article 26.

several roles, as they may be a unique data controller, a joint-controller, or a data processor for one data processing whereas carrying out another role for another data processing.

42. From a high-level perspective, the designer may act as a data controller when determining the purposes and means of a processing, but may intervene as a data processor when processing personal data on behalf of other parties, such as an application developer. The VVA user would therefore be subject to several data controllers: the application developer and the designer. It is also possible that the designer, the integrator and the developer are grouped into a single body acting as a unique data controller. In any case, the applicable qualifications have to be established on a case-by-case analysis.

> Example 1:
>
> The designer of the VVA processes user data for many purposes, including improving the VVA voice comprehension skills and respond accurately to requests. Therefore, and although this purpose may lead to the processing of data resulting from the use of applications provided by third parties, there is only one data controller: the designer of the VVA, on whose behalf and for whose purposes the processing is performed.

> Example 2:
>
> A bank offers to its customers an application that can be directly queried via the VVA in order to manage their accounts.
>
> Two actors are involved in the processing of personal data: the designer of the VVA and the developer of the banking application.
>
> In the scenario presented, the bank is the data controller for the provision of the service since it determines the purposes and essential means of processing related to the application allowing interaction with the assistant. Indeed, it offers a dedicated application that allows the user, a customer of the bank, to manage his/her accounts remotely. In addition, it decides on the means of processing by choosing appropriate processor, which is the designer of the VVA and can play an important role in assisting with its expertise to determining these means (for example, it can operate the development platform that allows third-party applications to be integrated into the VVA and, therefore, sets the framework and conditions to be respected by application developers).

43. On the data subject side, it is worth noting that several stakeholders may process the same personal data, even if the data subject does not really expect other parties than the VVA provider to be involved in the processing chain. So when a data subject acts with the VVA provider in relation to his/her personal data (e.g. exercise of data subject's rights), this does not automatically mean that this action will apply to the same personal data that is processed by another stakeholder. When these stakeholders are independent controllers, it is important that a clear information notice is given to the data subjects, explaining the various stages and actors of the processing. Moreover, in cases of joint controllership, it should be made clear if every controller is competent to comply with all data subject's rights or which controller is competent for which right.[20]

[20] Guidelines 7/2020, par. 165.

> Example 3:
>
> In this scenario, the designer of the VVA wishes to use the data collected and processed for the service provided by the bank in order to improve its voice recognition system. The designer of the VVA, who processes the data for its own purposes, will then have the status of controller for this specific processing.

44. As many stakeholders may be involved in the processing chain, and respectively many staff, risky situations may occur if no appropriate measures and safeguards are in place. Controllers are accountable for them and therefore should focus on protecting personal data, notably by choosing appropriate business partners and data processors, applying privacy by default and by design principles,[21] implementing adequate security and other GDPR tools such as audits and legal agreements (e.g. Articles 26 for joint controllers or 28 GDPR for processors).

45. VVA ecosystem is a complex one, where potentially many actors could exchange and process personal data as data controllers or processors. It is of utmost importance to clarify the role of each actor in respect of each processing and to follow the data minimisation principle also in respect of the data exchange.

46. In addition, controllers should be vigilant on personal data transfers and guarantee the required level of protection throughout the processing chain, in particular when they use services located outside of the EEA.

3.3 Transparency

47. Since VVAs process personal data (e.g. users' voice, location or the content of the communication), they must comply with the transparency requirements of the GDPR as regulated in Article 5 (1) (a) as well as Article 12 and Article 13 (enlightened by Recital 58). Data controllers are obliged to inform users of the processing of their personal data in a concise, transparent, intelligible form, and in an easily accessible way.

48. Failure to provide necessary information is a breach of obligations that may affect the legitimacy of the data processing. Complying with the transparency requirement is an imperative, since it serves as a control mechanism over the data processing and allows users to exercise their rights. Informing users properly on how their personal data is being used makes more difficult for data controllers to misuse the VVA for purposes that go far beyond user expectations. For example, patented technologies aim to infer health status and emotional states from a user's voice and adapt the services provided accordingly.

49. Complying with the transparency requirements can be particularly difficult for the VVA service provider or any other entity acting as data controller. Given the specific nature of VVAs, data controllers face several obstacles to comply with the GDPR's transparency requirements:

- **Multiple users**: data controllers should inform all users (registered, non-registered and accidental users), not only the user setting up the VVA.

[21] See EDPB 4/2019 Guidelines on Article 25 Data Protection by Design and by Default, Version 2.0, adopted on 20 October 2020.

- **Ecosystem complexity**: as explained in the technology background section, the identities and roles of those processing personal data when using a VVA is far from evident for the users.
- **Specificities of the vocal interface**: digital systems are not yet fit for voice-only interactions as the almost systemic use of a companion screen proves. However, adapting to the vocal interface and being able to inform the user clearly and correctly through this means is a necessity.

50. VVAs can be regarded as finite states machines going through a number of states during their ordinary functioning. They can be listening locally for the detection of wake-up expressions, or interacting with a remote server to resolve a command, but they can assume many other states depending on the context (e.g. if there is background environmental sound) or the user talking to them (e.g. they may talk to an identified or unknown user). Unfortunately, these situations take place in a substantial asymmetry of information with the user, who is hardly aware if the device is listening, and even less on the status in which it lies.

51. It is highly recommended that VVA designers and developers take adequate steps to fill those asymmetries, making the functioning of VVAs more interactive. Users should be informed of the status in which the device currently lies. This enhancement in transparency can be achieved both making the dialogue man-machine more interactive (e.g. the device might acknowledge in some way the reception of a vocal command), or broadcasting the status of the machine with specific signals. There are many options that can be explored in this regard, ranging from the use of specific vocal acknowledgements and visible icons or lights, or the use of displays on the device.

52. These issues are especially relevant considering the plurality of users and the presence among them of vulnerable categories of individuals, such as children, elderly people or users with audio-visual disabilities.

53. Two important questions become evident from the issues above: what is it the most feasible way to inform users and when is the appropriate time to inform them? These issues should be further examined in two different situations, depending on whether the VVA has only one user (such as a personal smart phone) or potentially multiple users (e.g. smart home device). Using the VVA technology, a subversion of these two basic settings could also occur, e.g. when a user has a personal smart phone and connects this to a car. The VVA of the smart phone, which could reasonably be expected to be used by that user only, is now "extended" to the others in the car.

54. Currently, all VVAs are connected to a user account and/or are set up by an application that requires one. The question of how data controllers could consider informing these users about the privacy policy while setting up the VVA should be addressed as described in the Article 29 Working Party Guidelines on transparency. Apps should make the necessary information available in an online store prior to download[22]. This way the information is given the earliest time possible and at the latest, at the time the personal data is obtained. Some VVA providers include third-party apps in the VVA default setup so these apps can execute those apps by using specific wake up expressions. VVAs using this third-party app deployment strategy should ensure that users get the necessary information also on the third-party processing.

[22] Guidelines on transparency under Regulation 2016/679, WP260 rev. 01, endorsed by EDPB (hereinafter "WP29 Guidelines WP260"), paragraph 11.

55. However, many VVA designers require VVA user accounts that bundle the VVA service with multiple other services like email, video streaming or purchases to name a few. The decision by the VVA designer of linking the account to many different services has the effect of requiring very lengthy and complex privacy policies. The length and complexity of such privacy policies greatly hinder fulfilling the transparency principle.

> Example 4:
>
> A VVA designer requires its users to have an account to access the VVA service. This user account is not specific to the VVA service and can be used for other services offered by the VVA designer such as email, cloud storage and social media. To create the account, users have to read and accept a 30 pages long privacy policy. The policy includes information on the processing of personal data by all the services that could be linked with the account.
>
> The information provided by the VVA designer in this case should not be deemed as concise and its complexity reduces the required transparency. Therefore, the VVA designer would not be complying with the transparency requirements as set out in Articles 12 and 13 GDPR.

56. Although the most common way to provide necessary information is in writing, the GDPR allows "other means" as well. Recital 58 explicitly states that the information can be given in electronic form, e.g. through a website. In addition, when choosing the appropriate method to inform the data subjects, account should be taken to the specific circumstances, such as the manner the data controller and the data subject otherwise interact with each other.[23] An option for devices without a screen could be to provide a link which is easy to understand, either directly or in an e-mail. Already existing solutions could serve as example for the information, e.g. call centres' practices of notifying the caller about a phone call being recorded and directing them to their privacy policies. The constraints of screen less VVA does not exempt the data controller from providing the necessary information according to the GDPR when setting up the VVA or installing or using a VVA app. VVA providers and developers should develop voice-based interfaces to facilitate the mandatory information.

57. VVAs could be of great interest for users with impaired vision since they provide an alternative interaction means with the IT services that traditionally rely on visual information. According to Article 12 (1) GDPR providing the necessary information orally is possible exclusively if requested so by the data subject, but not as the default method. However, the constraints of screen less VVAs would require automated oral information means that could be augmented by written means. When using audio to inform data subjects, data controllers should provide the necessary information in a way that is concise and clear. Furthermore, data subjects should be able to re-listen[24].

58. Taking the appropriate measures to comply with GDPR transparency requirements is more complex when there are multiple users of the VVA other than the owner of the device. VVA designers must consider how to properly inform non-registered and accidental users when their personal data is processed. When consent is the legal basis for processing users' data, users must be properly informed for the consent to be valid [25].

[23] WP29 Guidelines WP260, paragraph 19.
[24] WP29 Guidelines WP260, paragraph 21.
[25] GDPR, Article 4 (11).

59. In order to comply with the GDPR, data controllers should find a way to inform not only registered users, but also non-registered users and accidental VVA users. These users should be informed at the earliest time possible **and <u>at the latest, at the time of</u>** the processing. This condition could be especially difficult to fulfil in practice.

60. Certain corporate specificities should also not be detrimental to the data subjects. As many stakeholders are global companies or are well known for a specific business activity (e.g. telecommunication, e-commerce, information technologies, web activities), the way they provide a VVA service should be clear. Adequate information should make the data subjects understand whether or not their use of the VVA will be linked to other processing activities managed by the VVA service provider (e.g. telecommunication, e-commerce, information technologies or web activities) apart from the strict use of the VVA.

> Example 5:
>
> To use its assistant, a VVA designer which also provides a social media platform and a search engine, requires the user to link his/her account to the assistant. By linking his/her account to the use of the VVA, the designer can thus enhance the profile of its users through the use of the assistant, the applications (or skills) that are installed, the orders placed, etc. Hence assistant interactions are a new source of information attached to a user. VVA designer should provide users' with clear information as to how their data will be processed for each service and with controls allowing the user to choose if the data will be used or not for profiling.

Recommendations

61. When users are informed about the VVA processing of personal data using a user account's privacy policy and the account is linked to other independent services (e.g. email or online purchases), the EDPB recommends the privacy policy to have a clearly separated section regarding the VVA processing of personal data.

62. The information provided to the user should match the exact collection and processing that is carried out. While some meta-information is contained in a voice sample (e.g. stress level of the speaker), it is not automatically clear, whether such analysis is performed. It is crucial that controllers are transparent on what specific aspects of the raw data they process.

63. Furthermore it should at all times be apparent which state the VVA is in. Users should be able to determine whether a VVA is currently listening on its closed-loop circuit and especially whether it is streaming information to its back-end. This information should also be accessible for people with disabilities such as colour blindness (daltonism), deafness (anaccousia). Specific care should be given to the fact that VVAs suggest a usage scenario where eye-contact to the device is not necessary. So, all user feedback, including state changes should be available in visual and acoustic form at least.

64. Particular consideration should be applied if devices allow adding third party functionality ("apps" for VVAs). While some general information can be given to the user when they are the ones adding such functionality (given that it is the user's choice), during normal use of the device, the boundaries between the various controllers involved can be much less clear, i.e. the user might be not sufficiently informed how and by whom their data is processed (and to which extent) in a specific query.

65. All information about processing based on data collected and derived from the processing of recorded voice should also be available to users according to article 12 GDPR.

66. VVA controllers should make transparent what kind of information a VVA can derive about its surroundings, such as but not limited to other people in the room, music running in the background, any processing of the voice for medical or marketing other reasons, pets, etc.

3.4 Purpose limitation and legal basis

67. The processing of voice requests by VVAs has an evident purpose, the execution of the request. However, there often are additional purposes which are not so evident, like the improvement of the VVA natural language understanding capacities by training VVA model with machine learning techniques. Among the most common purposes for processing personal data by VVAs we find:

- Execute users' requests
- VVA improvement by training of the machine learning model and human review and labelling of voice transcriptions
- User identification (using voice data)
- User profiling for personalized content or advertising

68. Due to their role as intermediaries and the way they are designed, VVAs process a wide variety of personal and non-personal data. This allows processing personal data for many purposes that go beyond answering the users' requests and that could go totally unnoticed. By analysing data collected via VVAs, it is possible to know or infer user interests, schedules, driving routes or habits. This could enable personal data processing for unforeseen purposes (e.g. sentiment analysis or health condition assessment[26]), which would be far beyond the reasonable user expectations.

69. Data controllers should clearly specify their purpose(s) in relation to the context in which the VVA is used, so that they are clearly understood by the data subjects (e.g. presenting purposes in categories). In line with Article 5(1) GDPR, the personal data should be collected for specific, explicit and legitimate purposes and not further processed in a manner that is incompatible with these purposes.

3.4.1 Execute users' requests

70. The main use for a VVA is to issue voice commands that need to be executed by the VVA or an associated app or service (e.g. a music streaming service, a mapping service or an electronic lock). The user's voice and potentially other data (e.g. the user's position when requesting a route for a certain destination) might therefore be processed.

> Example 6:
>
> The passenger of a smart car including a VVA requests a route to the closest gas station. The VVA processes the user voice to understand the command and the car's position to find the route and sends it to the smart component to show it in the car's screen.

71. Insofar as the processing of voice commands involves the storage or access to information stored in the terminal devices of the end-user, Article 5(3) of the e-Privacy Directive must be

[26] Eoghan Furey, Juanita Blue, "Alexa, Emotion, Privacy and GDPR", Conference paper, Human Computer Interaction Conference, July [2018].

complied with. While Article 5(3) includes the general principle that such storage or access requires the prior consent of the end-user, it also provides for an exemption to the consent requirement where it is "strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service". Insofar as the voice data is processed in order to execute the user's requests, it is exempted from the requirement of prior consent.

72. As indicated earlier, any processing operations of personal data subsequent to the storage or access to information in the terminal device of end-users must have a legal basis under Article 6 GDPR to be lawful.

73. There are two consecutive processing operations taking place on the VVA. As mentioned above the first one requires access to the VVA (and therefore the conditions of Article 5(3) e-Privacy Directive must be met). In addition to the conditions of Article 5(3) e-Privacy Directive, this second step also requires a legal basis under Article 6 GDPR.

74. When an individual takes the decision to use a VVA, this action generally implies that the initial user first needs to register an account to activate the VVA. In other words, this situation refers to a contractual relationship[27] between the registered user and the VVA controller. In view of its substance and fundamental objective, the core purpose of this contract is to use the VVA in order to execute the user's request of assistance.

75. Any personal data processing that is necessary to execute the user's request can therefore rely on the legal basis of the performance of the contract[28]. Such processing notably includes the capture of the user's voice request, its transcription to text, its interpretation, the information exchanged with knowledge sources to prepare the reply and then, the transcription to a vocal final reply that ends the user's request.

76. Performance of a contract can be a legal basis for processing personal data using machine learning (ML) when it is necessary for the provision of the service. Processing personal data using ML for other purposes which are not necessary such as service improvement should not rely on that legal basis.

77. Last but not least, the legal bases of the performance of the contract and consent under the GDPR should not be confused. The consent provided for entering into, i. e. agreeing to the contract is part of the validity of this contract and does not refer to the specific meaning of the consent under the GDPR[29].

78. When using a VVA does not require to previously configure a user account to the VVA, consent could be a possible legal basis.

3.4.2 Improve the VVA by training the ML systems and manually reviewing of the voice and transcripts

79. The accents and variations of human speech are vast. While all VVAs are functional once out of the box, their performance can improve by adjusting them to the specific characteristics of

[27] Provided that "*the contract is valid pursuant to applicable national contract laws*", extract from Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects ("Guidelines 2/2019"), §26.
[28] In accordance with the Guidelines 2/2019, which moreover states that the Opinion 06/2014 remains relevant to Article 6(1)(b) and the GDPR (see in particular pages 11, 16, 17, 18 and 55 in this Opinion 06/2014).
[29] See Guidelines 2/2019, respectively §18, §19, §20, §21 and §27.

users' speech. As mentioned in section 2.6, this adjustment process relies on machine learning methods and consists of two processes: adding to the VVA training dataset new data collected from its users and the human review of the data processed for the execution of a fraction of the requests.

> Example 7:
>
> A VVA user has to issue three times the same voice command due to the VVA not understanding it. The three voice commands and the associated transcriptions are passed to human reviewers to review and correct the transcriptions. The voice commands and reviewed transcriptions are added to the VVA training dataset to improve its performance.

80. The processing activities described in the example should not be considered as (strictly) "*necessary for the performance of a contract*" within the meaning of Article 6(1)(b) GDPR, and therefore require another legal basis from Article 6 GDPR. The main reason being that VVAs are already functional when they come out of the box and can already perform as (strictly) necessary for the performance of the contract. The EDPB does not consider that Article 6(1)(b) would generally be an appropriate lawful basis for processing for the purposes of improving a service or developing new functions within an existing service. In most cases, a user enters into a contract to avail of an existing service. While the possibility of improvements and modifications to a service may routinely be included in contractual terms, such processing usually cannot be regarded as being objectively necessary for the performance of the contract with the user.

3.4.3 User identification[30] (using voice data)

81. The use of voice data for user identification implies the processing of biometric data as defined in Article 4.14 of the GDPR. Consequently, the data controller will need to identify an exemption under Article 9 of the GDPR in addition to the identification of a legal basis under Article 6 of the GDPR[31].

82. Of the exemptions listed in Article 9 of the GDPR, only data subjects' explicit consent seems applicable for this specific purpose.

83. However, since this purpose requires to apply the specific legal regime of article 9 of the GDPR further details follow in the section 3.8, related to the processing of special categories of data.

3.4.4 User profiling for personalized content or advertising

84. As mentioned above, VVAs have access to the content of all voice commands even when they are aimed at services provided by third parties. This access would enable the VVA designer to

[30] Technically, the notion of identification has to be distinguished from verification (authentication). Identification is a one-to-many (1: N) search and comparison and requires in principle a database in which several individuals are listed. Differently, the processing for verification purposes is a one-to-one (1:1) comparison and is used to verify and to confirm by a biometric comparison whether an individual is the same person as the one from whom the biometric data originates. To the knowledge of the EDPB, VVA on the market rely on the sole use of speaker identification technologies.

[31] GDPR considers that the mere nature of data is not always sufficient to determine if it qualifies as special categories of data since "*the processing of photographs […] are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person*" (recital 51). The same reasoning applies to voice.

construct very accurate user profiles that could be used to offer personalized services or advertisements.

> Example 8:
>
> Each time a VVA user makes an Internet search, the VVA adds labels signalling topics of interest to the user profile. The results for each new search are presented to the user ordered taking into account those labels.
>
> Example 9:
>
> Each time a VVA user makes a purchase from an e-commerce service, the VVA stores a record of the purchase order. The VVA provider enables third parties to target the VVA user with targeted advertisements on the basis of past purchases.

85. Personalisation of content may (but does not always) constitute an intrinsic and expected element of a VVA. Whether such processing can be regarded as an intrinsic aspect of the VVA service will depend on the precise nature of the service provided, the expectations of the average data subject in light not only of the terms of service but also the way the service is promoted to users, and whether the service can be provided without personalisation.[32]

86. Where personalisation takes place in the context of a contractual relationship and as part of a service explicitly request by the end-user (and the processing is limited to what is strictly necessary to provide this service), such processing may be based on article 6(1)(b) of the GDPR.

87. If processing is not strictly "*necessary for the performance of a contract*" within the meaning of Article 6(1)(b) GDPR, the VVA provider must, in principle, seek the consent of the data subject. Indeed, because consent will be required under Article 5(3) of the e-Privacy directive for the storing or gaining of access to information (see paragraphs 28-29 above), consent under Article 6(1)(a) GDPR will also, in principle, be the appropriate legal basis for the processing of personal data following those operations as reliance on legitimate interest could, in certain cases, risk undermining the additional level of protection provided by Article 5(3) of the e-Privacy directive.

88. Regarding user profiling for advertisement, it should be noted that this purpose is never considered as a service explicitly requested by the end-user. Thus, in case of processing for this purpose users' consent should be systematically collected.

Recommendations

89. Users should be informed of the purpose of processing personal data and that purpose should accord with their expectations of the device they purchase. In case of a VVA, that purpose – from a user's point of view – clearly is the processing of their voice for the sole purpose of interpreting their query and provide meaningful responses (be that answers to a query or other reactions like remote-controlling a light switch).

90. When the processing of personal data is based on consent, such consent "*should be given in relation to one or more specific purposes and that a data subject has a choice in relation to each of them*". Moreover, "*a controller that seeks consent for various different purposes should provide a separate opt-in for each purpose, to allow users to give specific consent for specific purposes*"[33]. For example, users should be able to separately consent or not for the manual review and labelling of voice transcriptions or the use of their voice data for user identification/authentication (see section 3.7).

[32] See also Guidelines 2/2019, paragraph 57.

3.5 Processing of children's data

91. Children can also interact with the VVAs or can create their own profiles connected to the ones of the adults. Some VVAs are embedded in devices which are specifically aimed at children.

92. When the legal basis for the processing is the performance of a contract, the conditions for processing children data will depend on national contract laws.

93. When the legal basis for the processing is consent and according to Article 8(1) GDPR, processing of children's data is only lawful "*where the child is at least 16 years old. Where the child is below the age of 16 years, such processing should be lawful only if and to the extent that consent is given or authorized by the holder of parental responsibility over the child*". Consequently, to comply with the GDPR, when consent is the legal basis, explicit permission should be sought from parents or guardians to collect, process, and store children's data (voice, transcripts, etc.).

94. Parental controls are available to a certain degree but in their current form they are not user friendly (e.g. it is necessary to sign in a new service) or have limited capacities. Data controllers should invest in developing means for parents or guardians to control children use of VVAs.

3.6 Data retention

95. VVAs process and generate a wide variety of personal data like voice, transcriptions of voice, metadata or system logs. These types of data could be processed for a wide range of purposes like provision of a service, NLP improvement, personalization or scientific research. Following the GDPR data storage limitation principle, VVAs should store data for no longer than is necessary for the purposes for which the personal data are processed. Therefore, the data retention periods should be tied to different processing purposes. VVA service providers or third-parties providing services through VVAs should assess the maximum retention period for each data set and purpose.

96. The data minimization principle is closely related to the data storage limitation principle. Not only do data controllers need to limit the data storage period, but also the type and quantity of data.

97. Data controllers should ask themselves, among others the following questions: Is it necessary to store all voice recordings or all transcriptions to achieve the purpose X? Is it necessary to store the voice data once the transcription has been stored? In that case, for what purpose? How long is voice or transcription data necessary for each purpose? The answer to these and other similar questions will define the retention periods that should be part of the information available to the data subjects.

98. Some VVA store by default personal data like voice snippets or transcriptions for an undefined period while providing users means to delete such data. Retaining personal data indefinitely goes against the storage limitation principle. Providing data subjects with means to delete

[33] See EDPB Guidelines 05/2020 on consent under Regulation 2016/679, adopted on 4 May 2020, section 3.2.

their personal data does not remove the data controller's responsibility of defining and enforcing a data retention policy.

99. VVA design needs to take into account users' controls to delete their personal data in their devices and in all remote storage systems. These controls may be required to resolve different kind of users' requests, for example, a request of erasure or the withdrawal of previously given consent. The design of some VVAs did not take into account this requirement.[34]

100. As in other contexts, data controllers may need to retain personal data as evidence of a service provided to a user to comply with a legal obligation. The data controller may retain personal data based on that basis. However, the data retained should remain the minimum necessary to comply with such a legal obligation and for the minimum amount of time. Of course, the data retained for the purpose of complying with a legal obligation should not be used for any other purposes without a legal basis under Article 6 GDPR.

> Example 10:
>
> A user purchases a TV in an e-commerce service using a voice command issued to a VVA. Even if the user requests afterwards the deletion of their data, the VVA provider or developer could still retain some data on the grounds of their legal obligation set by tax regulation to keep purchase evidence. However, the data stored for this purpose should not exceed the minimum necessary to comply with the legal obligation and could not be processed for any other purposes without a legal basis under Article 6 GDPR.

101. As mentioned in section 2, VVAs voice recognition capacity improves by training machine learning systems with users' data. If users do not consent or withdraw their consent to the use of their data for such purpose, their data could not be lawfully used to train any more model and should be deleted by the data controller, assuming that there is no other purpose justifying the continued retention. However, there is evidence that there may be risks of re-identification in some machine learning models.[35]

102. Data controllers and processors should use models which do not restrict their ability to stop processing if an individual revokes their consent, nor should they use models which restrict their ability to facilitate data subject rights. Controllers and processors should apply mitigation measures to reduce the re-identification risk to an acceptable threshold.

103. In the event that the user withdraws his or her consent, the data collected from the user can no longer be used for further training of the model. Nevertheless, the model previously trained using this data does not have to be deleted. The EDPB however highlights that there is evidence that there may be risks of personal data leaking in some machine learning models In particular, numerous studies showed that reconstruction as well as membership inference attacks can be performed, allowing attackers to retrieve information about individuals.[36] Data controllers and processors should therefore apply mitigation measures to reduce the re-identification risk to an acceptable threshold to make sure they use models which do not contain personal data.

104. Data subjects should not be nudged to keep their data indefinitely. While deleting stored voice data or transcriptions might have an impact on the service performance, such impact should be explained to users in a clear and measurable way. VVA service providers should avoid making general statements on the degradation of the service after personal data is deleted.

105. Anonymizing voice recordings is specially challenging, as it is possible to identify users through the content of the message itself and the characteristics of voice itself. Nevertheless, some research[37] is being conducted on techniques that could allow to remove situational information like background noises and anonymize the voice.

Recommendations

106. From a user's perspective, the main purpose of processing their data is querying and receiving responses and/or triggering actions like playing music or turning on or off lights. After a query has been answered or a command executed, the personal data should be deleted unless the VVA designer or developer has a valid legal basis to retain them for a specific purpose.

107. Before considering anonymization as means for fulfilling the data storage limitation principle, VVA providers and developers should check the anonymization process renders the voice unidentifiable.

108. Configuration defaults should reflect these requirements by defaulting to an absolute minimum of stored user information. If these options are presented as part of a setup wizard, the default setting should reflect this, and all options should be presented as equal possibilities without visual discrimination.

109. When during the review process the VVA provider or developer detects a recording originated on a mistaken activation, the recording and all the associated data should be immediately deleted and not used for any purpose.

3.7 Security

110. To securely process personal data, VVAs should protect their confidentiality, integrity and availability. Apart from risks stemming from elements on the VVA ecosystem, using voice as communication means creates a new set of security risks.

111. VVAs are multiuser. They may allow for more than one registered user and anyone on their surroundings can issue commands and use their services. Any VVA service requiring confidentiality will involve some access control mechanism and user authentication. Without access control, anyone able to issue voice commands to the VVA could access, modify or delete any users' personal data it (e.g. ask for received messages, user's address or calendar events). Issuing voice commands to the VVA does not require being physically close to it since they can

[34] See Amazon's letter of 28 June 2019 in response to US Senator Christopher Coons: https://www.coons.senate.gov/imo/media/doc/Amazon%20Senator%20Coons__Response%20Letter__6.28.19[3].pdf

[35] Veale Michael, Binns Reuben and Edwards Lilian 2018 "Algorithms that remember: model inversion attacks and data protection law" Phil. Trans. R. Soc. A.37620180083, doi: 10.1098/rsta.2018.0083

[36] N. Carlini et al, "Extracting Training Data from Large Language Models" Dec 2020.

[37] See, for example, VoicePrivacy (https://www.voiceprivacychallenge.org), an initiative to develop privacy preservation solutions for speech technology.
See also open-source voice anonymization tools developed by H2020 research and innovation project COMPRISE: https://gitlab.inria.fr/comprise/voice_transformation.

be manipulated, for example, via signal broadcasting[38] (e.g. radio or TV). Some of the known methods to remotely issue commands to VVAs like laser[39] or ultrasonic (inaudible) waves[40]are not even detectable by human senses.

112. User authentication can rely on one or more of the following factors: something you know (such as a password), something you have (such as a smart card) or something you are (such as a voice fingerprint). A closer look at these authentication factors in the VVA context shows that:

- Authentication using something the user knows is problematic. The secret that would allow users to prove their identity should be spoken aloud, exposing it to anyone in the surroundings. VVAs communication channel is the surrounding air, a channel type that cannot be fortified in the way traditional channels are (e.g. by limiting the access to the channel or encrypting its content).
- Authentication using something the user has would require the VVA service providers to create, distribute and manage "tokens" that could be used as proof of identity.
- Authentication using something the user is implies the use of biometric data for the purpose of uniquely identifying a natural person (see section 3.7 below).

113. VVA user accounts are associated to the devices in which the service is provided. Often the same account used to manage the VVA is used to manage other services. For example, owners of an Android mobile phone and a Google Home speaker can and most likely associate their Google account to both devices. Most VVAs do not require or offer an identification or authentication mechanism when a device providing a VVA service has just one user account.

114. When there is more than one user account associated with the device, some VVAs offer an optional basic access control in the form of PIN number with no real user authentication. Some other VVAs have the option to use voice fingerprint recognition as identification mechanism.

115. Although user identification or authentication might not be necessary to access all VVA services, it will definitely be for some. Without an identification or authentication mechanism, anyone could access other users' data and modify or erase them at will. For example, anyone close to a smart speaker could delete other users' playlists from the music streaming service, commands from the command history or contacts from the contact list.

116. Most VVAs blindly trust their local networks. Any compromised device in the same network could change the settings of the smart speaker or allow the installation of malware or to associate fake apps/skills to it without the user's knowledge or agreement.[41]

[38] X. Yuan et al., "All Your Alexa Are Belong to Us: A Remote Voice Control Attack against Echo" 2018 IEEE Global Communications Conference (GLOBECOM), Abu Dhabi, United Arab Emirates, 2018, pp. 1-6, doi: 10.1109/GLOCOM.2018.8647762.
[39] See, for example, https://lightcommands.com
[40] See, for example, https://surfingattack.github.io
[41] See, for example, Deepak Kumar et al., *Skill Squatting Attacks on Amazon Alexa*, USENIX Security Symposium, August 2018, https://www.usenix.org/conference/usenixsecurity18/presentation/kumar
Security Research Labs, *Smart Spies: Alexa and Google Home expose users to vishing and* eavesdropping, November 2019, https://srlabs.de/bites/smart-spies

117. VVAs, like any other software, are subject to software vulnerabilities. However, due to the VVA market concentration[42] any vulnerability could affect millions of VVA users. If working as currently designed, VVAs do not send any information to the speech recognition cloud service until the wake-up expression is detected. However, software vulnerabilities could allow an attacker to bypass the VVA set-up and security measures. It could then be possible for example to get a copy of all data sent to the VVA cloud and forward it to a server controlled by the attacker.

118. Data lawfully processed or derived by VVAs allow building a fairly accurate profile of their users as VVA know or can infer the location, the relations and the interests of their users. VVAs are increasingly present in users' homes and smartphones. This circumstance increases the risk of mass surveillance and mass profiling. Consequently, the security measures to protect the data both in transit and at rest, in the devices and in the Cloud, should match those risks.

119. The increasing use of VVA in conjunction with not adequately balanced access rights by law enforcement authorities could induce a chilling effect that would undermine fundamental rights like freedom of speech.

120. Law enforcement authorities, both in[43] and out[44] of the EU, have already expressed their interest in accessing the voice snippets captured by VVAs. Access to data processed or derived by VVAs in the EU should comply with the existing EU data protection and privacy regulation framework. In case some Member States consider issuing specific legislation restricting the fundamental rights to privacy and data protection, such restrictions should always comply with the requirement set out in Article 23 of the GDPR[45].

121. The human review of voice recordings and associated data to improve VVA service quality is a common practice among VVA providers. Due to the sensitive nature of the data that is processed by this human reviewers and the fact that this process is often subcontracted to a processors, it is of utmost relevance that adequate security measures are put in place.

Recommendations

122. VVA designers and application developers should provide secure state-of-the-art authentication procedures to users.

123. Human reviewers should always receive the strictly necessary pseudonymised data. The legal agreements governing the review should expressly forbid any processing that could lead to the identification of the data subject.

124. If emergency calling is provided as a service through the VVA, a stable uptime[46] should be guaranteed.

3.8 Processing of special categories of data

125. As previously mentioned, VVAs have access to information of an intimate nature which can be protected under article 9 of the GDPR (see section 3.7.1), such as biometric data (see section

[42] The VVA market is currently shared among less than a dozen service providers.
[43] See, for example, https://www.ft.com/content/ad765972-87a2-11e9-a028-86cea8523dc2.
[44] See, for example, https://cdt.org/insights/alexa-is-law-enforcement-listening.
[45] See also EDPB, Guidelines 10/2020 on restrictions under Article 23 GDPR.
[46] The time a device or a service can be left unattended without crashing, or needing to be rebooted for administrative or maintenance purposes.

3.7.2). Therefore, VVA designers and developers must carefully identify in which cases the processing implies special categories of data.

3.8.1 General considerations when processing special categories of data

126. VVAs may process special categories of data in different circumstances:

- As part of their own services, for example when managing medical appointments in users' agendas.
- When acting as interface for third-party services, VVA providers process the content of the commands. Depending on the type of service requested by the user, VVA providers could process special categories of data. An example could be when a user issues commands to a VVA to use a third-party app used to keep track of her ovulation.[47]
- When voice data is used for the purpose of uniquely identify the user, as developed below.

3.8.2 Specific considerations when processing biometric data

127. Some VVA have the capability of uniquely identifying their users merely based on their voice. This process is known as voice model recognition. During the enrolment phase of voice recognition, the VVA processes a user's voice to create a voice model (or voiceprint). During its regular use, the VVA can calculate the voice model of any users and compare it to the enrolled models to uniquely identify the user who executed a command.

> Example 11:
>
> A group of users set up a VVA to use voice model recognition. After doing so, each of them enrol their voice models.
>
> Later, a user requests the VVA access to the meetings in his or her agenda. Since access to the agenda requires user identification, the VVA extracts the model from the request's voice, calculates its voice model and checks if it matches an enrolled user and if that specific user has access to the agenda.

128. In the example above, the recognition of a the user's voice on the basis of a voice model amounts to the processing of special categories of personal data within the meaning of Article 9 GDPR (processing of biometric data for the purpose of uniquely identifying a natural person).[48] The processing of biometric data for the purpose of user identification as required in the example will require the explicit consent of the data subject(s) concerned (Article 9(2)(a) GDPR). Therefore, when obtaining users' consent, data controllers must comply with the conditions of Article 7 and as clarified in recital 32 of the GDPR and should offer an alternative identification method to biometrics, with regard to the free nature of consent.

129. When using voice data for biometric identification or authentication, data controllers are required to make transparent where biometric identification is used and how voiceprints (biometric models) are stored and propagated across devices. To fulfil this transparency requirement, the EDPB recommends to provide the answers to the following questions:

- Does the activation of voice identification on one device automatically activate this feature on all other devices running with the same account?
- Does the activation of voice identification propagate through the VVA controller's infrastructure to devices owned by other users?
- Where are biometric models generated, stored and matched?
- Are biometric models accessible to VVA providers, developers or others?

130. When the registered user configures the VVAs to identify the voice of its users, the voice of non-registered and accidental users will also be processed for the purpose of uniquely identifying them.

131. Indeed, detecting the voice of the right speaker also involves comparing it with that of other people in the assistant's vicinity. In other words, the speaker recognition functionality implemented in voice assistants may require the voice biometrics of people speaking in the household to be recorded, to allow the user's voice characteristics to be distinguished from those of the person who wishes to be recognised. Biometric identification may therefore have the consequence of subjecting uninformed persons to biometric processing, by registering their model and comparing it with that of the user wishing to be recognised.

132. In order to avoid such collection of biometric data without the knowledge of the data subjects while allowing a user to be recognized by the assistant, solutions based on the user's data alone should be given priority. In concrete terms, this means that biometric recognition is only activated at each use at the user's initiative, and not by a permanent analysis of the voices heard by the assistant. For instance, a specific keyword or question to the persons present could be provided in order to obtain their consent to trigger biometric processing. For example, the user can say "identification" or the assistant can ask "do you wish to be identified" and wait for a positive response to activate biometric processing.

> Example 12:
>
> If the user wishes to set up biometric authentication for access to certain protected data such as his/her bank account, the voice assistant could activate speaker verification, when he/she launches the application only, and verify his/her identity in this way.

Recommendations

133. Voice models should be generated, stored and matched exclusively on the local device, not in remote servers.

134. Due to the sensitiveness of the voiceprints, standards such as ISO/IEC 24745 and techniques of biometric model protection[49] should be thoroughly applied.

[47] See for example, a product available here: https://www.amazon.com/Ethan-Fan-Ovulation-Period-Tracker/dp/B07CRLSHKY

[49] See for example:
Jain, Anil & Nandakumar, Karthik & Nagar, Abhishek. (2008). "*Biometric Template Security*". EURASIP Journal on Advances in Signal Processing. 2008. 10.1155/2008/579416.
S. K. Jami, S. R. Chalamala and A. K. Jindal, "*Biometric Template Protection Through Adversarial Learning*" *2019 IEEE International Conference on Consumer Electronics (ICCE)*, Las Vegas, NV, USA, 2019, pp. 1-6, doi: 10.1109/ICCE.2019.8661905.

135. If a VVA uses voice based biometric identification VVA providers should:

- Ensure that the identification is accurate enough to reliably associate personal data to the right data subjects.
- Ensure that the accuracy is similar for all user groups by checking that there is no substantial bias towards different demographic groups.

3.9 Data minimization

136. Controllers should minimize the amount of data that is collected directly or indirectly and obtained by processing and analysis, e.g. not perform any analysis on the user's voice or other audible information to derive information about their mental state, possible disease or circumstances of their life.

137. Roll out settings by default that limit any data collecting and/or processing to a minimum required amount needed to provide the service.

138. Depending on the location, use context and microphone sensitivity, VVA could collect third parties' voice data as part of the background noise when collecting the users' voice. Even if background noise does not include voice data, it can still include situational data that could be processed to derive information about the subject (e.g. location).

Recommendations

139. VVA designers should consider technologies deleting the background noise to avoid recording and processing background voices and situational information.

3.10 Accountability

140. For any processing that is based on consent, controllers are obliged to be able to prove the consent of data subjects according to Article 7 (1) GDPR. Voice data can be used for accountability (e.g. to prove consent). The retention obligation for such voice data would then be dictated by the accountability requirements of the relevant specific legislation.

141. When evaluating the need for a Data Protection Impact Assessment (DPIA), the EDPB set out criteria[50] to be used by data protection authorities in creating lists of processing operations that require a mandatory DPIA and provide examples of processing that are likely to require a DPIA. It is very likely that VVA services fall into the categories and conditions identified as needing a DPIA. This includes considering if the device may be observing monitoring or controlling data subjects or systematically monitoring at large scale as per Article 35(3)(c), use of "new technology", or the processing of sensitive data and data concerning vulnerable data subjects.

142. All data collection and processing activities must be documented in accordance with Article 30 GDPR. That includes all processing involving voice data.

[50] Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA), wp248, rev.01, endorsed by EDPB.

Recommendations

143. If voice messages are to be used to inform users according to Article 13, the data controllers should publish such messages on their website so they are accessible to the users and the data protection authorities.

3.11 Data protection by design and by default

144. VVA providers and developers should consider the necessity of having a registered user for each of their functionalities. While it is clear that it is necessary to have a registered user to manage an agenda or an address book, it is not so clear that making a phone call or an Internet search requires the VVA to have a registered user.

145. By default, services which do not require an identified user should not associate any of the VVA identified users to the commands. A privacy and data protection friendly default VVA would only process users' data for executing users' requests and would store neither voice data nor a register of executed commands.

146. While some devices can only run one VVA, others can choose among different VVAs. VVA providers should develop industry standards enabling data portability in accordance with Article 20 of the GDPR.

147. Some VVA providers alleged their VVAs could not delete all users' data even when requested by the data subject. VVA providers should ensure that all users' data can be erased at the user's request in accordance with Article 17 of the GDPR.

4 MECHANISMS TO EXERCISE DATA SUBJECT RIGHTS

148. In compliance with the GDPR, data controllers providing VVA services must allow all users, registered and non-registered, to exercise their data subject rights.

149. VVA providers and developers should facilitate data subjects' control over their data during the entire processing period, in particular ease their right of access, rectification, erasure, their right to restrict the processing and, depending on the legal basis of the processing, their right to data portability and their right to object.

150. The data controller should provide information on the data subject's rights at the time when data subjects switch on a VVA and at the latest, at the time when the first user's voice request is processed.

151. Given that the main interaction means for VVAs is voice, VVA designers should ensure that users, registered or not, can exercise any data subject rights, using easy-to-follow voice commands. VVA designers, as well as app developers in case they are part of the solution, should at the end of the exercise process inform the user that his/her rights have been duly factored, by voice or by providing a writing notification to the user's mobile, account or any other mean chosen by the user.

152. At least, VVA designers and app developers, notably, should implement specific tools providing an effective and efficient way to exercise such rights. They should therefore propose for their devices, a way to exercise data subjects' rights as by providing the data subject with self-

service tools, as a profile management system[51]. This could facilitate an efficient and timely handling of data subject's rights and will enable the data controller to include the identification mechanism in the self-service tool.

153. In regards of the exercise of data subjects rights in case of multiple users, when a user, registered or not, exercises one of his or her rights, he or she should do so without prejudice to any other users' rights. All the users, registered and non-registered can exercise their rights as long as the data controller is still processing the data. Data controller should set up a process ensuring that data subject rights are exercised.

4.1 Right to access

154. According to Article 12(1) GDPR, communication under Article 15 should be provided in writing, or by other means, including, where appropriate, by electronic means. As regards access to the personal data undergoing processing, Article 15(3) states that where the data subject makes the request by electronic means, and unless otherwise requested by the data subjects, the information should be provided in a commonly used electronic form. What could be considered as a commonly used electronic form should be based upon the reasonable expectations of the data subjects and not upon what format the data controller uses in its daily operations. The data subject should not be obliged to buy specific software or hardware in order to get access to the information.

155. On demand, data controllers should therefore send a copy of personal data, and audio data (including voice recordings and transcriptions) in particular, in a common format readable by the data subject.

156. When deciding about the type of format the information under Article 15 should be provided in, the data controller needs to keep in mind that the format should enable the information to be presented in a way that is both intelligible and easy accessible. Data controllers should also tailor the information to the specific situation of the data subject making the request.

> Example 13:
>
> A data controller providing a VVA service receives, from a user, both a request of access and a request for data portability. The data controller decides to provide the information under both Article 15 and Article 20 in a PDF file. In such a case, the data controller should not be considered to handle both requests in a correct manner. A PDF file technically fulfils the obligations on the data controller under Article 15, but does not fulfil the obligations on the data controller under Article 20.[52]
>
> It should be noted that simply referring users to a history of their interactions with the voice assistant does not appear to enable the data controller to meet all its obligations under the right of access, as the accessible data generally represents only part of the information processed in the context of providing the service.

[51] Profile management system is understood as a place within the VVA system, where users may, anytime, store its preferences, set modification and change easily his/her privacy settings
[52] WP29 Guidelines on the right to data portability - endorsed by the EDPB, p. 18.

157. The right of access should not be used to counter / to get around the principles of minimisation and data retention.

4.2 Right to rectification

158. To facilitate data rectification, users, registered or not, should be able to manage and update, at any time, their data by voice directly from the VVA device, as described above. Furthermore self-service tool should be implemented inside the device or an application in order to help them to rectify easily their personal data. Users should be notified by voice, or by writing of the update.

159. More generally, the right to rectification applies to any opinions and inferences[53] of the data controller, including profiling, and should consider the vast majority of data is highly subjective.[54]

4.3 Right to erasure

160. Users, registered or not, should be able, at any time, by voice from the VVA device, or from a self-service tool integrated into any device associated to the VVA, to delete data concerning them. In this respect, the personal data can be deleted by a data subject as easily as it is submitted. Due to the inherent difficulties of anonymising voice data and the wide variety of personal data collected from, observed and inferred about the data subject,[55] in this context the right to erasure could be hardly accommodated by anonymising personal datasets. As the GDPR is technology neutral and technology evolves rapidly, it will nevertheless not be excluded that right to erasure may be made effective through anonymization.

161. In some cases, without a third party screen or the possibility of displaying data stored (e.g. a mobile application or a tabular device), it is difficult to have a preview of the recorded tracks, to judge the relevance of the suggestions. A dashboard (or an application) widely accessible to users in order to ease its use should be supplied with the voice assistant to delete the history of the requests asked and customize the tool according to user's needs.[56]

162. For any data processing and, in particular, when registered data subjects consent to the voice recordings to be transcribed and used by the provider for the improvement of its services, VVA providers should, on demand of the user, be able to delete the initial voice recording as well as any related transcription of the personal data.

163. The data controller should ensure that no more processing may occur, after the exercise of the right of erasure. In regards to previous actions, the right to erasure may meet some legal and technical limits, notably.

[53] The fact that opinions and inferences can qualify as personal data has been confirmed by the CJEU, which noted that the term 'any information' in the definition of personal data includes information that is 'not only objective but also subjective, in the form of opinions and assessments, provided that it 'relates' to the data subject' - Case C-434/16 *Peter Nowak v Data Protection Commissioner* ECLI:EU:C:2017:994 [34].
[54] Getting Data Subject Rights Right, A submission to the EDPB from data protection academics, November 2019.
[55] Article 29 Working Party Opinion 05/2014 on Anonymisation Techniques, adopted on 10 April 2014.
[56] "Assistants vocaux et enceintes connectées, l'impact de la voix sur l'offre et les usages culturels et médias", the French "Conseil Supérieur de l'Audiovisuel", May 2019.

Example 14:

If prior to the deletion request, a user made an online purchase by means of his/her VVA, the VVA provider may delete the voice recording relating to the online purchase and ensure no more future further use. However, the purchase will still be effective as well as the vocal order or the written transcription processed by the e-commerce website (here the exemption is based of legal obligation of the e-commerce website).

In the same vein, if prior to the deletion request, the user added a specific song to his/her playlist, by means of his/her VVA, the VVA providers will be able to delete the oral request, but not the past consequences of such request (the erasure will not impact the user's playlist).

164. Based on the above, in case the same personal data is processed for different processing purposes, data controllers should interpret erasure requests as a clear signal to stop processing of the data for all purposes that are not legally exempted.

In accordance with the conditions set out in Article 21(1) of the GDPR, data processed on the basis of legitimate interests of the VVA providers should not be an exemption to the right of erasure, in particular, because data subjects do not reasonably expect further processing of their personal data.

4.4 Right to data portability

165. The data processing made by the VVA providers falls under the scope of data portability, as processing operations are mainly based, on the data subject's consent (under Article 6(1)(a), or under Article 9(2)(a) when it comes to special categories of personal data) or, on a contract to which the data subject is a party under Article 6(1)(b).

166. In practice, the right to data portability should facilitate switching between different VVA providers. VVAs operating in a digital environment in particular and data subject's voice being recorded in an application or a platform, the right to data portability should be granted for all personal data provided by the data subject. Furthermore, the data controller should offer users the possibility of directly retrieving their personal data from their user area, as a self-service tool. The users should also be able to exercise this right through voice command.

167. VVA providers and developers should give to the data subjects an extensive control over the personal data concerning him or her, in order to allow them to transfer personal data from a VVA provider to another. Data subjects should, therefore, receive his/her personal data provided to the data controller, in a structured, commonly used and machine-readable format as well as from means[57] that contribute to answer data portability requests (such as download tools and Application Programming Interfaces)[58]. As stated in the Guidelines on the right to data portability, in case of large or complex personal data collection, that could be the case here, the data controller should provide an overview "*in a concise, transparent, intelligible and easily accessible form, using clear and plain language*" (see Article 12(1) of the GDPR) in such a way that data subjects should always have clear information of what data to download or transmit to another data controller in relation to a given purpose. For example, data subjects should be in a position to use software applications to easily identify, recognize and process specific data from it.

168. This right should allow the user to retrieve for his/her personal use, the data that he/she has communicated by means of his/her voice (e.g. the history of voice interactions) and within the framework of the creation of his/her user account (e.g.: name and first name), notably.

169. For the full application of this data subjects' right in a context of one digital single market, VVA designers and app developers, notably, should develop common machine-readable formats that ease interoperability of the data format between VVA systems[59], including the standard formats for voice data. Technologies should be structured in order to ensure that personal data, including voice data, processed are easily and fully reusable by the new controller[60].

170. In regards to the format, VVA providers should provide personal data using commonly used open formats (e.g. mp3, wav, csv, gsm, etc.) along with suitable metadata used in order to accurately describe the meaning of exchanged information.[61]

5 ANNEX: AUTOMATIC SPEECH RECOGNITION, SPEECH SYNTHESIS AND NATURAL LANGUAGE PROCESSING

171. Following the theoretical foundations of signal processing, notably Claude Shannon's information and sampling theories, automatic speech processing has become a fundamental component of engineering sciences. At the crossroads of physics (acoustics, wave propagation), applied mathematics (modelling, statistics), computer science (algorithms, learning techniques) and human sciences (perception, reasoning), speech processing has rapidly been broken down into numerous subjects of study: speaker identification and verification, automatic speech recognition, voice synthesis, emotion detection, etc. Over the last fifteen years or so, the discipline as a whole has made very significant progress, with various factors contributing to this: improved methods, a significant increase in computing capacities and greater volumes of data available.

[57] See as an illustration, the reasoning of the Article 29 Working Party in the Guidelines on the right to data portability - endorsed by the EDPB, p. 16:
"*On a technical level, data controllers should explore and assess two different and complimentary paths for making portable data available to the data subjects or to other data controllers:*
- a direct transmission of the overall dataset of portable data (or several extracts of parts of the global dataset);
- an automated tool that allows extraction of relevant data.
The second way may be preferred by data controllers in cases involving of complex and large data sets, as it allows for the extraction of any part of the data-set that is relevant for the data subject in the context of his or her request, may help minimizing risk, and possibly allows for use of data synchronization mechanisms (e.g. in the context of a regular communication between data controllers). It may be a better way to ensure compliance for the "new" data controller, and would constitute good practice in the reduction of privacy risks on the part of the initial data controller".

[58] In this respect: Article 29 Working Party Guidelines on the right to data portability - endorsed by the EDPB, p. 1.

[59] In this respect: recital (68) of the GDPR; WP29 Guidelines on the right to data portability - endorsed by the EDPB, p. 17.

[60] "*In this respect, recital 68 encourages data controllers to develop interoperable formats that enable data portability but without creating an obligation for controllers to adopt or maintain processing systems which are technically compatible. The GDPR does, however, prohibit controllers from establishing barriers to the transmission*" - WP29 Guidelines on the right to data portability - endorsed by the EDPB, p. 5.

[61] EDPB strongly encourages cooperation between industry stakeholders and trade associations to work together on a common set of interoperable standards and formats to deliver the requirements of the right to data portability.

5.1 Automatic Speech Recognition (ASR)

172. The automatic speech recognition (also known as speech to text) used to involve three distinct stages aimed at: 1) determine which phonemes were said using an acoustic model; 2) determine which words were said using a phonetic dictionary; 3) transcribe the sequence of words (sentence) most likely to have been said using a language model. Today, with the progress made possible by deep learning (a machine learning technique), many systems offer "end to end" automatic speech recognition. This avoids the need to go through the complex training of three different models while offering better performance in terms of results and processing time. Almost all major digital players now offer their own ASR implementations that can be easily used by API systems, but open-source systems also exist (DeepSpeech[62] or Kaldi[63] for example).

5.2 Natural Language Processing (NLP)

173. Natural Language Processing is a multidisciplinary field involving linguistics, computer science and artificial intelligence, which aims to create natural language processing tools for a variety of applications. The fields of research and applications are numerous: syntactic analysis, machine translation, automatic text generation and summarization, spell checking, question answering systems, text mining, named entity recognition, sentiment analysis, etc. Concretely, NLP's goal is to give computers the ability to read, understand and derive meaning from human languages. The development of NLP applications is challenging because computer tools traditionally require humans to interact with them in a programming language that is formal, meaning precise, unambiguous and highly structured. Human speech, however, is not always precise. It is often ambiguous and the linguistic structure can depend on many complex variables, including slang, regional dialects and social context.

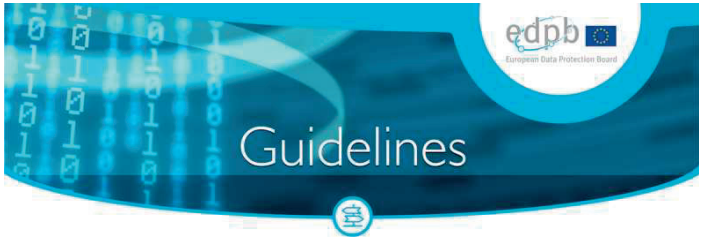
174. Syntax and semantic analysis are two main techniques used with NLP. Syntax is the arrangement of words in a sentence to make grammatical sense. NLP uses syntax to assess meaning from a language based on grammatical rules. Syntax techniques used include parsing (grammatical analysis for a sentence), word segmentation (which divides a large piece of text to units), sentence breaking (which places sentence boundaries in large texts), morphological segmentation (which divides words into groups) and stemming (which divides words with inflection in them to root forms). Semantics involves the use and meaning behind words. NLP applies algorithms to understand the meaning and structure of sentences. Techniques that NLP uses with semantics include word sense disambiguation (which derives meaning of a word based on context), named entity recognition (which determines words that can be categorized into groups), and natural language generation (which will use a database to determine semantics behind words). While earlier approaches to NLP involved rules-based approaches, where simple machine learning algorithms were told what words and phrases to look for in text and given specific responses when those phrases appeared, current approaches to NLP are based on deep learning, a type of AI that examines and uses patterns in data to improve a program's understanding.

5.3 Speech Synthesis

175. Speech synthesis is the artificial production of human speech. Speech synthesis has mainly been implemented by concatenation of vocal units that are stored in a database. This technique consists in selecting, from all the recordings of an actor previously transcribed into phonemes, syllables and words, the bricks of sound that correspond to the words that one wishes to have pronounced by the VVA and to assemble them one after the other to form an intelligible sentence with natural diction. Alternatively, a speech synthesizer can incorporate a model of the vocal tract and other human voice characteristics in order to model the parameters of a voice such as intonation, rhythm, and timbre, by generative statistical models (such as WaveNet[64], Tacotron[65] or DeepVoice[66]) and to create a completely synthetic voice output.

[62] https://github.com/mozilla/DeepSpeech
[63] https://github.com/kaldi-asr/kaldi

[64] Aäron van den Oord et Sander Dieleman, *WaveNet: A generative model for raw audio*, Deepmind blog, september 2016, https://deepmind.com/blog/article/wavenet-generative-model-raw-audio
[65] Yuxuan Wang, *Expressive Speech Synthesis with Tacotron*, Google AI blog, March 2018, https://ai.googleblog.com/2018/03/expressive-speech-synthesis-with.html
[66] *Deep Voice 3: 2000-Speaker Neural Text-to-Speech*, Baidu Research blog, October 2017 http://research.baidu.com/Blog/index-view?id=91



Guidelines 01/2021

on Examples regarding Data Breach Notification

Adopted on 14 January 2021

Version 1.0

Table of contents

1 Introduction 4
2 RANSOMWARE 7
2.1 **CASE No. 01: Ransomware with proper backup and without exfiltration** 7
2.1.1 CASE No. 01 - Prior measures and risk assessment 7
2.1.2 CASE No. 01 – Mitigation and obligations 8
2.2 **CASE No. 02: Ransomware without proper backup** 9
2.2.1 CASE No. 02 - Prior measures and risk assessment 9
2.2.2 CASE No. 02 – Mitigation and obligations 10
2.3 **CASE No. 03: Ransomware with backup and without exfiltration in a hospital** 11
2.3.1 CASE No. 03 - Prior measures and risk assessment 11
2.3.2 CASE No. 03 – Mitigation and obligations 11
2.4 **CASE No. 04: Ransomware without backup and with exfiltration** 12
2.4.1 CASE No. 04 - Prior measures and risk assessment 12
2.4.2 CASE No. 04 – Mitigation and obligations 12
2.5 Organizational and technical measures for preventing / mitigating the impacts of ransomware attacks 13
3 Data Exfiltration ATTACKS 14
3.1 **CASE No. 05: Exfiltration of job application data from a website** 14
3.1.1 CASE No. 05 - Prior measures and risk assessment 15
3.1.2 CASE No. 05 – Mitigation and obligations 15
3.2 **CASE No. 06: Exfiltration of hashed password from a website** 16
3.2.1 CASE No. 06 - Prior measures and risk assessment 16
3.2.2 CASE No. 06 – Mitigation and obligations 16
3.3 **CASE No. 07: Credential stuffing attack on a banking website** 17
3.3.1 CASE No. 07 - Prior measures and risk assessment 17
3.3.2 CASE No. 07 – Mitigation and obligations 17
3.4 Organizational and technical measures for preventing / mitigating the impacts of hacker attacks. 18
4 INTERNAL HUMAN RISK SOURCE 19
4.1 **CASE No. 08: Exfiltration of business data by a former employee** 19
4.1.1 CASE No. 08 - Prior measures and risk assessment 19
4.1.2 CASE No. 08 – Mitigation and obligations 20
4.2 **CASE No. 09: Accidental transmission of data to a trusted third party** 20
4.2.1 CASE No. 09 – Prior measures and risk assessment 20

4.2.2 CASE No. 09 – Mitigation and obligations 21
4.3 Organizational and technical measures for preventing / mitigating the impacts of internal human risk sources 21
5 LOST OR STOLEN DEVICES AND PAPER DOCUMENTS 22
5.1 **CASE No. 10: Stolen material storing encrypted personal data** 23
5.1.1 CASE No. 10 - Prior measures and risk assessment 23
5.1.2 CASE No. 10 – Mitigation and obligations 23
5.2 **CASE No. 11: Stolen material storing non-encrypted personal data** 24
5.2.1 CASE No. 11 - Prior measures and risk assessment 24
5.2.2 CASE No. 11 – Mitigation and obligations 24
5.3 **CASE No. 12: Stolen paper files with sensitive data** 24
5.3.1 CASE No. 12 – Prior measures and risk assessment 24
5.3.2 CASE No. 12 – Mitigation and obligations 25
5.4 Organizational and technical measures for preventing / mitigating the impacts of loss or theft of devices 25
6 MISPOSTAL 26
6.1 **CASE No. 13: Snail mail mistake** 26
6.1.1 CASE No. 13 - Prior measures and risk assessment 26
6.1.2 CASE No. 13 – Mitigation and obligations 26
6.2 **CASE No. 14: Sensitive personal data sent by mail by mistake** 27
6.2.1 CASE No. 14 - Prior measures and risk assessment 27
6.2.2 CASE No. 14 – Mitigation and obligations 27
6.3 **CASE No. 15: Personal data sent by mail by mistake** 27
6.3.1 CASE No. 15 - Prior measures and risk assessment 27
6.3.2 CASE No. 15 – Mitigation and obligations 28
6.4 **CASE No. 16**: Snail mail mistake 28
6.4.1 CASE No. 16 - Prior measures and risk assessment 29
6.4.2 CASE No. 16 – Mitigation and obligations 29
6.5 Organizational and technical measures for preventing / mitigating the impacts of mispostal 29
7 Other Cases – Social Engineering 30
7.1 **CASE No. 17**: Identity theft 30
7.1.1 CASE No. 17 - Risk assessment, mitigation and obligations 30
7.2 **CASE No. 18: Email exfiltration** 31
7.2.1 CASE No. 18 - Risk assessment, mitigation and obligations 31

THE EUROPEAN DATA PROTECTION BOARD

Having regard to Article 70 (1e) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, (hereinafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018[1],

Having regard to Article 12 and Article 22 of its Rules of Procedure,

Having regard to the Communication from the Commission to the European Parliament and the Council titled Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation[2],

HAS ADOPTED THE FOLLOWING GUIDELINES

1 INTRODUCTION

1. The GDPR introduces the requirement for a personal data breach to be notified to the competent national supervisory authority (hereinafter "SA") and, in certain cases, to communicate the breach to the individuals whose personal data have been affected by the breach (Articles 33 and 34).
2. The Article 29 Working Party already produced a *general* guidance on data breach notification in October 2017, analysing the relevant Sections of the GDPR (Guidelines on Personal data breach notification under Regulation 2016/679, WP 250) (hereinafter "Guidelines WP250)[3]. However, due to its nature and timing, this guideline did not address all practical issues in sufficient detail. Therefore, the need has arisen for a *practice-oriented, case-based* guidance that utilizes the experiences gained by SAs since the GDPR is applicable.
3. This document is intended to complement the Guidelines WP 250 and it reflects the common experiences of the SAs of the EEA since the GDPR became applicable. Its aim is to help data controllers in deciding how to handle data breaches and what factors to consider during risk assessment.

[1] References to "Member States" made throughout this document should be understood as references to "EEA Member States".

[2] COM(2020) 264 final, 24 June 2020.

[3] G29 WP250 rev.1, 6 February 2018, Guidelines on Personal data breach notification under Regulation 2016/679 - endorsed by the EDPB, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052.

4. As part of any attempt to address a breach the controller should first be able to recognize one. The GDPR defines a "personal data breach" in Article 4(12) as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".

5. In its Opinion 03/2014 on breach notification[4] and in its Guidelines WP 250, WP29 explained that breaches can be categorised according to the following three well-known information security principles:

    - "Confidentiality breach" - where there is an unauthorised or accidental disclosure of, or access to, personal data.
    - "Integrity breach" - where there is an unauthorised or accidental alteration of personal data.
    - "Availability breach" - where there is an accidental or unauthorised loss of access to, or destruction of, personal data[5].

6. A breach can potentially have a range of significant adverse effects on individuals, which can result in physical, material, or non-material damage. The GDPR explains that this can include loss of control over their personal data, limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymization, damage to reputation, and loss of confidentiality of personal data protected by professional secrecy. It can also include any other significant economic or social disadvantage to those individuals. One of the most important obligation of the data controller is to evaluate these risks to the rights and freedoms of data subjects and to implement appropriate technical and organizational measures to address them.

7. Accordingly, the GDPR requires the controller to:

    - document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken[6];
    - notify the personal data breach to the supervisory authority, unless the data breach is unlikely to result in a risk to the rights and freedoms of natural persons[7];

[4] G29 WP213, 25 March 2014, Opinion 03/2014 on Personal Data Breach Notification, p. 5, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm#maincontent5ec4.

[5] See Guidelines WP 250, p. 7.

[6] GDPR Article 33(5).

[7] GDPR Article 33(1).

    - communicate the personal data breach to the data subject when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons[8].

8. Data breaches are problems in and of themselves, but they are also symptoms of a vulnerable, possibly outdated data security regime, thus indicate system weaknesses to be addressed. As a general truth, it is always better to prevent data breaches by preparing in advance, since several consequences of them are by nature irreversible. Before a controller can *fully* assess the risk arising from a breach caused by some form of attack, the root cause of the issue should be identified, in order to identify whether any vulnerabilities that gave rise to the incident are still present, and are still therefore exploitable. In many cases the controller is able to identify that the incident is likely to result in a risk, and is therefore to be notified. In other cases the notification does not need to be postponed until the risk and impact surrounding the breach has been fully assessed, since the full risk assessment can happen in parallel to notification, and the information thus gained may be provided to the SA in phases without undue further delay[9].

9. The breach should be notified when the controller is of the opinion that it is likely to result in a risk to the rights and freedoms of the data subject. Controllers should make this assessment at the time they become aware of the breach. The controller should not wait for a detailed forensic examination and (early) mitigation steps before assessing whether or not the data breach is likely to result in a risk and thus should be notified.

10. If a controller self-assesses the risk to be unlikely, but it turns out that the risk materializes, the relevant SA can use its corrective powers and may resolve to sanctions.

11. Every controller should have plans, procedures in place for handling eventual data breaches. Organisations should have clear reporting lines and persons responsible for certain aspects of the recovery process.

12. Training and awareness on data protection issues of the staff of the controller focusing on personal data breach management (identification of a personal data breach incident and further actions to be taken, etc.) is also essential for the controllers. This training should be regularly repeated, depending on the type of the processing activity and size of the controller, addressing latest trends and alerts coming from cyberattacks or other security incidents.

13. The principle of accountability and the concept of data protection by design could incorporate analysis that feeds into a data controller's own "Handbook on Handling Personal Data Breach" that aims to establish facts for each facet of the processing at each major stage of the operation. Such a handbook prepared in advance would provide a much quicker source of information to allow data controllers to mitigate the risks and meet the obligations without undue delay. This would ensure that if a personal data breach was to occur, people in the organisation would know what to do, and the incident would more than likely be handled quicker than if there were no mitigations or plan in place.

14. Though the cases presented below are fictitious, they are based on typical cases from the SA's collective experience with data breach notifications. The analyses offered relate explicitly to the cases

[8] GDPR Article 34(1).

[9] GDPR Article 33(4).

under scrutiny, but with the goal to provide assistance for data controllers in assessing their own data breaches. Any modification in the circumstances of the cases described below may result in different or more significant levels of risk, thus requiring different or additional measures. These guidelines structure the cases according to certain categories of breaches (e.g. ransomware attacks). Certain mitigating measures are called for in each case when dealing with a certain category of breaches. These measures are not necessarily repeated in each case analysis belonging to the same category of breaches. For the cases belonging to the same category only the differences are laid out. Therefore, the reader should read all cases relevant to relevant category of a breach to identify and distinguish all the correct measures to be taken.

15. The internal documentation of a breach is an obligation independent of the risks pertaining to the breach, and must be performed in each and every case. The cases presented below try to shed some light on whether or not to notify the breach to the SA and communicate it to the data subjects affected.

2 RANSOMWARE

16. A frequent cause for a data breach notification is a ransomware attack suffered by the data controller. In these cases a malicious code encrypts the personal data, and subsequently the attacker asks the controller for a ransom in exchange for the decryption code. This kind of attack can usually be classified as a breach of availability, but often also a breach of confidentiality could occur.

2.1 CASE No. 01: Ransomware with proper backup and without exfiltration

Computer systems of a small manufacturing company were exposed to a ransomware attack, and data stored in those systems was encrypted. The data controller used encryption at rest, so all data accessed by the ransomware was stored in encrypted form using a state-of-the-art encryption algorithm. The decryption key was not compromised in the attack, i.e. the attacker could neither access it nor use it indirectly. In consequence, the attacker only had access to encrypted personal data. In particular, neither the email system of the company, nor any client systems used to access it were affected. The company is using the expertise of an external cybersecurity company to investigate the incident. Logs tracing all data flows leaving the company (including outbound email) are available. After analysing the logs and the data collected by the detection systems the company has deployed, an internal investigation supported by the external cybersecurity company determined *with certainty* that the perpetrator only encrypted data, without exfiltrating it. The logs show no outward data flow in the timeframe of the attack. The personal data affected by the breach relates to clients and employees of the company, a few dozen individuals altogether. A backup was readily available, and the data was restored a few hours after the attack took place. The breach did not result in any consequences on the day-to-day operation of the controller. There was no delay in employee payments or handling client requests.

17. In this case the following elements were realized from the definition of a "personal data breach": a breach of security led to unlawful alteration and unauthorized access to personal data stored.

2.1.1 CASE No. 01 - Prior measures and risk assessment

18. As with all risks posed by external actors, the likelihood that a ransomware attack is successful can be drastically reduced by tightening the security of the data controlling environment. The majority of these breaches can be prevented by ensuring that appropriate organizational, physical and technological security measures have been taken. Examples of such measures are proper patch management and the use of an appropriate anti-malware detection system. Having a proper and separate backup will help to

mitigate the consequences of a successful attack should it occur. Moreover, an employee security education, training, and awareness (SETA) program, will help to prevent and recognise this kind of attack. (A list of advisable measures can be found in section 2.5) Among those measures, a proper patch management that ensures that the systems are up to date and all known vulnerabilities of the deployed systems are fixed is one of the most important since most of the ransomware attacks exploit well-known vulnerabilities.

19. When assessing the risks, the controller should investigate the breach and identify the type of the malicious code to understand the possible consequences of the attack. Among those risks to be considered is the risk that data was exfiltrated without leaving a trace in the logs of the systems.

20. In this example, the attacker had access to personal data and the confidentiality of cipher text containing personal data in encrypted form was compromised. However, any data that might have been exfiltrated cannot be read or used by the perpetrator, at least for the time being. The encryption technique used by the data controller conforms to the state-of-the-art. The decryption key was not compromised and presumably could also not be determined by other means. In consequence, the confidentiality risks to the rights and freedoms of natural persons are reduced to a minimum barring cryptanalytic progress that renders the encrypted data intelligible in the future.

21. The data controller should consider the impact and severity of the breach. In this case, it appears the risks to the rights and freedoms of data subjects result from the lack of availability of the personal data, and the confidentiality of the personal data is not compromised[10]. In this example, the adverse effects of the breach were mitigated fairly soon after the breach occurred. Having a proper backup regime[11] makes the effects of the breach less severe and here the controller was able to effectively make use of it.

22. On the severity of the consequences for the data subjects, only minor consequences could be identified since the affected data was restored in a few hours, the breach did not result in any consequences on the day-to-day operation of the controller and had no significant effect on the data subjects (e.g. employee payments or handling client requests).

2.1.2 CASE No. 01 – Mitigation and obligations

23. Without a backup few measures to remediate the loss of personal data can be undertaken by the controller, and the data has to be collected again. In this particular case however, the impacts of the attack could effectively be contained by resetting all compromised systems to a clean state known to be free of malicious code, fixing the vulnerabilities and restoring the affected data soon after the attack.

[10] Technically, encryption of data will involve "access" to original data, and in the case of ransomware, the deletion of the original – the data needs to be accessed by ransomware code to encrypt it, and to remove the original data. An attacker may take a copy of the original before deletion, but personal data will not always be extracted. As a data controller's investigation progresses, new information may come to light to make this assessment change. Access that results in unlawful destruction, loss, alteration, unauthorised disclosure of the personal data, or to a security risk to a data subject, even without interpretation of the data may be as severe as access with interpretation of the personal data.

[11] Backup procedures should be structured, consistent and repeatable. Examples of back up procedures are the 3-2-1 method and the grandfather-father-son method. Any method should always be tested for effectiveness in coverage and when data is to be restored. Testing should also be repeated at intervals and especially when changes occur in the processing operation or its circumstances to ensure the integrity of the system.

Without a backup, data is lost and the severity may increase because risks or impacts to individuals may also do so.

24. The timeliness of an effective data restoration from the readily available backup is a key variable when analysing the breach. Specifying an appropriate timeframe to restore the compromised data depends on the unique circumstances of the breach at hand. The GDPR states that a personal data breach shall be notified without undue delay and, where feasible, not later than after 72 hours. Therefore, it could be determined that exceeding the 72-hour time limit is unadvisable in any case, but when dealing with high risk level cases, even complying with this deadline can be viewed as unsatisfactory.

25. In this case, following a detailed impact assessment and incident response process, the controller determined that the breach was unlikely to result in a risk to the rights and freedoms of natural persons, hence no communication to the data subjects is necessary, nor does the breach require a notification to the SA. However, as all data breaches, it should be documented in accordance with Article 33 (5). The organisation may also need (or later be required by the SA) to update and remediate its organizational and technical personal data security handling and risk mitigation measures and procedures.

Actions necessary based on the identified risks		
No risk (internal register)	Risk (notify SA)	High Risk (communicate to data subjects)
✓	X	X

2.2 CASE No. 02: Ransomware without proper backup

One of the computers used by an agricultural company was exposed to a ransomware attack and its data was encrypted by the attacker. The company is using the expertise of an external cybersecurity company to monitor their network. Logs tracing all data flows leaving the company (including outbound email) are available. After analysing the logs and the data the other detection systems have collected the internal investigation aided by the cybersecurity company determined that the perpetrator only encrypted the data, without exfiltrating it. The logs show no outward data flow in the timeframe of the attack. The personal data affected by the breach relates to the employees and clients of the company, a few dozen individuals altogether. No special categories of data were affected. No backup was available in an electronic form. Most of the data was restored from paper backups. The restoration of the data took 5 working days and led to minor delays in the delivery of orders to customers.

2.2.1 CASE No. 02 - Prior measures and risk assessment

26. The data controller should have adopted the same prior measures as mentioned in part 2.1. and in section 2.9. The major difference to the previous case is the lack of an electronic backup and the lack of encryption at rest. This leads to critical differences in the following steps.

27. When assessing the risks, the controller should investigate the method of infiltration and identify the type of the malicious code to understand the possible consequences of the attack. In this example the ransomware encrypted the personal data without exfiltrating it. As a result, it appears the risks to the rights and freedoms of data subjects result from the lack of availability of the personal data, and the confidentiality of the personal data is not compromised. A thorough examination of the firewall logs and its implications is essential in determining the risk. The data controller should present the factual findings of these investigations upon request.

28. The data controller needs to keep in mind that if the attack is more sophisticated the malware has the functionality to edit log files and remove the trace. So - given that logs are not forwarded or replicated to a central log server - even after a thorough investigation that determined that the personal data was not exfiltrated by the attacker, the data controller cannot state that the absence of a log entry proves the absence of exfiltration, therefore the likelihood of a confidentiality breach cannot be entirely dismissed.

29. The data controller should assess the risks of this breach if the data was accessed by the attacker. During the risk assessment, the data controller should also take into consideration the nature, the sensitivity, the volume, and the context of personal data affected in the breach. In this case no special categories of personal data are affected, and the quantity of breached data and the number of affected data subjects is low.

30. Gathering exact information on the unauthorized access is key for determining the risk level and preventing a new or continued attack. If the data had been copied from the database, it would obviously have been a risk-increasing factor. When uncertain about the specifics of the illegitimate access, the worse scenario should be considered and the risk should be assessed accordingly.

31. The absence of a backup database can be considered a risk enhancing factor depending on the severity of consequences for the data subjects resulting from the lack of availability of the data.

2.2.2 CASE No. 02 – Mitigation and obligations

32. Without a backup few measures to remediate the loss of personal data can be undertaken by the controller, and the data has to be collected again, unless some other source is available (e.g. order confirmation e-mails). Without a backup, data may be lost and the severity will depend on the impact for the individuals.

33. The restoration of the data should not prove to be overly problematic[12] if the data is still available on paper, but given the lack of an electronic backup database, a notification to the SA is considered necessary, as the restoration of the data took some time and could cause some delays in the orders' delivery to customers and a considerable amount of meta-data (e.g. logs, time stamps) might not be retrievable.

34. Informing the data subjects about the breach may also depend on the length of time the personal data is unavailable and the difficulties it might cause in the operation of the controller as a result (e.g. delays in transferring employee's payments). As these delays in payments and deliveries may lead to financial loss for the individuals whose data has been compromised, one could also argue the breach is likely to result in a high risk. Also, it might not be possible to avoid informing the data subjects if their contribution is needed for restoring the encrypted data.

35. This case serves as an example for a ransomware attack with risk to the rights and freedoms of the data subjects, but not reaching high risk. It should be documented in accordance with Article 33 (5) and notified to the SA in accordance with Article 33 (1). The organisation may also need (or be required by

[12] This will depend on the complexity and structure of the personal data. In the most complex scenarios, re-establishing data integrity, consistency with metadata, ensuring the correct relationships within data structures and checking data accuracy may take significant resources and effort.

the SA) to update and remediate its organizational and technical personal data security handling and risk mitigation measures and procedures.

Actions necessary based on the identified risks		
No risk (internal register)	Risk (notify SA)	High Risk (communicate to data subjects)
✓	✓	✗

2.3 CASE No. 03: Ransomware with backup and without exfiltration in a hospital

The information system of a hospital / healthcare centre was exposed to a ransomware attack and a significant proportion of its data was encrypted by the attacker. The company is using the expertise of an external cybersecurity company to monitor their network. Logs tracing all data flows leaving the company (including outbound email) are available. After analysing the logs and the data the other detection systems have collected the internal investigation aided by the cybersecurity company determined that the perpetrator only encrypted the data without exfiltrating it. The logs show no outward data flow in the timeframe of the attack. The personal data affected by the breach relates to the employees and patients, which represented thousands of individuals. Backups were available in an electronic form. Most of the data was restored but this operation lasted 2 working days and led to major delays in treating the patients with surgery cancelled / postponed, and to a lowering the level of service due to the unavailability of the systems.

2.3.1 CASE No. 03 - Prior measures and risk assessment

36. The data controller should have adopted the same prior measures as mentioned in part 2.1. and in section 2.5. The major difference to the previous case is the high severity of consequences for a substantial part of the data subjects.

37. The quantity of breached data and the number of affected data subjects are high, because hospitals usually process large quantities of data. The unavailability of the data has a high impact on a substantial part of the data subjects. Moreover, there is a residual risk of high severity to the confidentiality of the patient data.

38. The type of the breach, nature, sensitivity, and volume of personal data affected in the breach are important. Even though a backup for the data existed and it could be restored in a few days, a high risk still exists due to the severity of consequences for the data subjects resulting from the lack of availability of the data at the moment of the attack and the following days.

2.3.2 CASE No. 03 – Mitigation and obligations

39. A notification to the SA is considered necessary, as special categories of personal data are involved and the restoration of the data could take a long time, resulting in major delays in patient care. Informing the data subjects about the breach is necessary due to the impact for the patients, even after restoring the encrypted data. While data relating to all patients treated in the hospital during the last years have been encrypted, only those patients who were scheduled to be treated in the hospital during the time the computer system was unavailable were impacted. The controller should communicate the data breach to those patients directly. Direct communication to the other patients some of which may not have been in the hospital for more than twenty years may not be required due to the exception in Article 34 (3) c). In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner. In this case, the hospital should make the ransomware attack and its effects public.

40. This case serves as an example for a ransomware attack with high risk to the rights and freedoms of the data subjects. It should be documented in accordance with Article 33 (5), notified to the SA in accordance with Article 33 (1) and communicated to the data subjects in accordance with Article 34 (1). The organisation also needs to update and remediate its organizational and technical personal data security handling and risk mitigation measures and procedures.

Actions necessary based on the identified risks		
No risk (internal register)	Risk (notify SA)	High Risk (communicate to data subjects)
✓	✓	✓

2.4 CASE No. 04: Ransomware without backup and with exfiltration

The server of a public transportation company was exposed to a ransomware attack and its data was encrypted. According to the findings of the internal investigation the perpetrator not only encrypted the data, but also exfiltrated it. The type of breached data was the personal data of clients and employees, and of the several thousand people using the services of the company (e.g. buying tickets online). Beyond basic identity data, identity card numbers and financial data such as credit card details are involved in the breach. A backup database existed, but it was also encrypted by the attacker.

2.4.1 CASE No. 04 - Prior measures and risk assessment

41. The data controller should have adopted the same prior measures as mentioned in part 2.1. and in section 2.5. Though backup was in place, it was also affected by the attack. This arrangement alone raises questions about the quality of the controller's prior IT security measures and should be further scrutinised during the investigation, since in a well-designed backup regime the backup has to be securely stored without access from the main system, otherwise it could be compromised in the same attack.

42. This breach concerns not only data availability, but confidentiality as well, since the attacker may have modified and / or copied data from the server. Therefore, the type of the breach results in high risk.

43. The nature, sensitivity, and volume of personal data increases the risks further, because the number of individuals affected is high, as is the overall quantity of affected personal data. Beyond basic identity data, identity documents and financial data such as credit card details are involved too. A data breach concerning these types of data presents high risk in and of themselves, and if processed together, they could be used for – among others - identity theft or fraud.

44. Due to either faulty server logic or organizational controls, the backup files were affected by the ransomware, preventing the restore of data and enhancing the risk.

45. This data breach presents a high risk to the rights and freedoms of individuals, because it could likely lead to both material (e.g. financial loss since credit card details were affected) and non-material damage (e.g. identity theft or fraud since identity card details were affected).

2.4.2 CASE No. 04 – Mitigation and obligations

46. Communication to the data subjects is essential, so they can make the necessary steps to avoid material damage (e.g. block their credit cards).

47. Aside from documenting the breach in accordance with Article 33 (5), a notification to the SA is also mandatory in this case (Article 33 (1)) and the controller is also obliged to communicate the breach to the data subjects (Article 34 (1)). The latter could be undertaken on a person-by-person basis, but for individuals where contact data is not available the controller should do so publicly, e.g. by way of a notification on its website. In the latter case a precise and clear communication is required, in plain sight on the homepage of the controller, with exact references of the relevant GDPR provisions. The organisation may also need to update and remediate its organizational and technical personal data security handling and risk mitigation measures and procedures.

Actions necessary based on the identified risks		
Internal documentation	Notification to SA	Communication to data subjects
✓	✓	✓

2.5 Organizational and technical measures for preventing / mitigating the impacts of ransomware attacks

48. The fact that a ransomware attack could have taken place is usually a sign of one or more vulnerabilities in the controller's system. This also applies in ransomware cases in which the personal data has been encrypted, but has not been exfiltrated. Regardless of the outcome and the consequences of the attack, the importance of an all-encompassing evaluation of the data security system - with particular emphasis on IT security - cannot be stressed enough. The identified weaknesses and security holes are to be documented and addressed without delay.

49. Advisable measures:

(*The list of the following measures is by no means exclusive or comprehensive. Rather, the goal is to provide prevention ideas and possible solutions. Every processing activity is different, hence the controller should make the decision on which measures fit the given situation the most.*)

- Keeping the firmware, operating system and application software on the servers, client machines, active network components, and any other machines on the same LAN (including Wi-Fi devices) up to date. Ensuring that all reasonable IT security measures are in place, making sure they are effective and keeping them regularly updated when processing or circumstances change or evolve. This includes keeping detailed logs of which patches are applied at which timestamp.
- Designing and organising processing systems and infrastructure to segment or isolate data systems and networks to avoid propagation of malware within the organisation and to external systems.
- The existence of an up-to-date, secure and tested backup procedure. Media for medium- and long-term back-up should be kept separate from operational data storage and out of reach of third parties even in case of a successful attack (such as daily incremental backup and weekly full backup).
- Having / obtaining an appropriate, up-to-date, effective and integrated anti-malware software.
- Having an appropriate, up-to-date, effective and integrated firewall and intrusion detection and prevention system. Directing network traffic through the firewall/intrusion detection, even in the case of home office or mobile work (e.g. by using VPN connections to organizational security mechanisms when accessing the internet).

- Training employees on the methods of recognising and preventing IT attacks. The controller should provide means to establish whether emails and messages obtained by other means of communication are authentic and trustworthy. Employees should be trained to recognize when such an attack has realized, how to take the endpoint out of the network and their obligation to immediately report it to the security officer.
- Emphasize the need of identifying the type of the malicious code to see the consequences of the attack and be able to find the right measures to mitigate the risk. In case a ransomware attack has succeeded and there is no back-up available, tools available such as the ones by the "no more ransom" (nomoreransom.org) project may be applied to retrieve data. However, in case a safe backup is available, restoring the data from it is advisable.
- Forwarding or replication all logs to a central log server (possibly including the signing or cryptographic time-stamping of log entries).
- Strong encryption and authentication, in particular for administrative access to IT systems (2FA), appropriate key and password management.
- Vulnerability and penetration testing on a regular basis.
- Establish a Computer Security Incident Response Team (CSIRT) or Computer Emergency Response Team (CERT) within the organization, or join a collective CSIRT/CERT. Create an Incident Response Plan, Disaster Recovery Plan and a Business Continuity Plan, and make sure that these are thoroughly tested.
- When assessing countermeasures – risk analysis should be reviewed.

3 DATA EXFILTRATION ATTACKS

50. Attacks that exploit vulnerabilities in services offered by the controller to third parties over the internet, e.g. committed by way of injection attacks (e.g. SQL injection, path traversal), website compromising and similar methods, may resemble ransomware attacks in that the risk emanates from the action of an unauthorized third party, but those attacks typically aim at copying, exfiltrating and abusing personal data for some malicious end. Hence, they are mainly breaches of confidentiality and, possibly, also data integrity. At the same time, if the controller is aware of the characteristics of this kind of breaches, there are many measures available to controllers that can substantially reduce the risk of a successful execution of an attack.

3.1 CASE No. 05: Exfiltration of job application data from a website

An employment agency was the victim of a cyber-attack, which placed a malicious code on its website. This malicious code made personal information submitted through online job application forms and stored on the webserver accessible to unauthorized person(s). 213 such forms are possibly affected, after analysing the affected data it was determined that no special categories of data were affected in the breach. The particular malware toolkit installed had functionalities that allowed the attacker to remove any history of exfiltration and also allowed processing on the server to be monitored and to have personal data captured. The toolkit was discovered only a month after its installation.

3.1.1 CASE No. 05 - Prior measures and risk assessment

51. The security of the data controller's environment is extremely important, as the majority of these breaches can be prevented by ensuring that all systems are constantly updated, sensitive data is encrypted and applications are developed according to high security standards like strong authentication, measures against brute force, attacks, "escaping" or "sanitising"[13] user inputs, etc. Periodic IT security audits, vulnerability assessments and penetration tests are also required in order to detect these kinds of vulnerabilities in advance and fix them. In this particular case, file integrity monitoring tools in production environment might have helped to detect the code injection. (A list of advisable measures is to be found in section 3.7).

52. The controller should always start to investigate the breach by identifying the type of the attack and its methods, in order to assess what measures are to be taken. To make it fast and efficient, the data controller should have an incident response plan in place which specifies the swift and necessary steps to take control over the incident. In this particular case, the type of the breach was a risk enhancing factor since not only was data confidentiality curtailed, the infiltrator also had the means to establish changes in the system, so data integrity also became questionable.

53. The nature, sensitivity and volume of personal data affected in the breach should be assessed to determine to what extent the breach affected the data subjects. Though no special categories of personal data were affected, the accessed data contains considerable information about the individuals from the online forms, and such data could be misused in a number of ways (targeting with unsolicited marketing, identity theft, etc.), so the severity of the consequences should increase the risk to the right and freedoms of the data subjects.

3.1.2 CASE No. 05 – Mitigation and obligations

54. If possible, after solving the problem, the database should be compared with the one stored in a secure backup. The experiences drawn from the breach should be utilized in updating the IT infrastructure. The data controller should return all affected IT systems to a known clean state, remedy the vulnerability and implement new security measures to avoid similar data breaches in the future, e.g. file integrity checks and security audits. If personal data was not only exfiltrated, but also deleted, the controller has to take systematic action to recover the personal data in the state it was in before the breach. It may be necessary to apply full backups, incremental changes and then possibly rerun the processing since the last incremental backup – which requires that the controller is able to replicate the changes made since the last backup. This could require that the controller has the system designed to retain the daily input files in case they need to be processed again and requires a robust method of storage and a suitable retention policy.

55. In light of the above, as the breach is likely to result in a high risk to the rights and freedoms of natural persons, the data subjects should definitely be informed about it (Article 34(1)), which of course means that the relevant SA(s) should also be involved in the form of a data breach notification. Documenting the breach is obligatory according to Article 33 (5) GDPR and makes the assessment of the situation easier.

[13] Escaping or sanitizing user inputs is a form of input validation, which ensures that only properly formatted data is entered into an information system.

Actions necessary based on the identified risks		
Internal documentation	Notification to SA	Communication to data subjects
✓	✓	✓

3.2 CASE No. 06: Exfiltration of hashed password from a website

An SQL Injection vulnerability was exploited to gain access to a database of the server of a cooking website. Users were only allowed to choose arbitrary pseudonyms as usernames. The use of email addresses for this purpose was discouraged. Passwords stored in the database were hashed with a strong algorithm and the salt was not compromised. Affected data: hashed passwords of 1.200 users. For safety's sake, the controller informed the data subjects about the breach via e-mail and asked them to change their passwords, especially if the same password was used for other services.

3.2.1 CASE No. 06 - Prior measures and risk assessment

56. In this particular case data confidentiality is compromised, but the passwords in the database were hashed with an up-to-date method, which would decrease the risk regarding the nature, sensitivity, and volume of personal data. This case presents no risks to the rights and freedoms of the data subjects.

57. Furthermore, no contact information (e.g. e-mail addresses or phone numbers) of data subjects was compromised, which means there is no significant risk for the data subjects of being targeted by fraud attempts (e.g. receiving phishing e-mails or fraudulent text messages and phone calls). No special categories of personal data were involved.

58. Some user names could be regarded as personal data, but the subject of the website does not allow for negative connotations. Although it has to be noted that the risk assessment may change, if the type of the website and the data accessed could reveal special categories of personal data (e. g. website of a political party or trade union). Using state of the art encryption could mitigate the adverse effects of the breach. Assuring that a limited number of attempts to login is allowed will prevent brute force login attacks to be successful, thus reducing largely the risks imposed by attackers already knowing the usernames.

3.2.2 CASE No. 06 – Mitigation and obligations

59. The communication to the data subjects in some cases could be considered a mitigating factor, since the data subjects are also in a position to make the necessary steps to avoid further damages from the breach, for example by changing their password. In this case, notification was not mandatory, but in many cases it can be considered a good practice.

60. The data controller should correct the vulnerability and implement new security measures to avoid similar data breaches in the future like, for example, systematic security audits to the website.

61. The breach should be documented in accordance with Article 33 (5) but no notification or communication needed.

62. Also, it is strongly advisable to communicate a breach involving passwords to data subjects in any case even when the passwords were stored using a salted hash with an algorithm conforming to the state-of-the-art. The use of authentication methods obviating the need to process passwords on the server side is preferable. Data subjects should be given the choice to take appropriate measures regarding their own passwords.

Actions necessary based on the identified risks		
Internal documentation	Notification to SA	Communication to data subjects
✓	✗	✗

3.3 CASE No. 07: Credential stuffing attack on a banking website

A bank suffered a cyber-attack against one of its online banking websites. The attack aimed to enumerate all possible login user IDs using a fixed trivial password. The passwords consist of 8 digits. Due to a vulnerability of the website, in some cases information regarding data subjects (name, surname, gender, date and place of birth, fiscal code, user identification codes) were leaked to the attacker, even if the used password was not correct or the bank account not active anymore. This affected around 100.000 data subjects. Out of these, the attacker successfully logged into around 2.000 accounts which were using the trivial password tried by the attacker. After the fact, the controller was able to identify all illegitimate log-on attempts. The data controller could confirm that, according to antifraud checks, no transactions were performed by these accounts during the attack. The bank was aware of the data breach because its security operations centre detected a high number of login requests directed toward the website. In response, the controller disabled the possibility to log in to the website by switching it off and forced password resets of the compromised accounts. The controller communicated the breach only to the users with the compromised accounts, i.e. to users whose passwords were compromised or whose data was disclosed.

3.3.1 CASE No. 07 - Prior measures and risk assessment

63. It is important to mention that controllers handling sensitive data, financial information, etc. have a larger responsibility in terms of providing adequate data security, e.g. having a security operation's centre and other incident prevention, detection and response measures. Not meeting these higher standards will certainly result in more serious measures during an SA's investigation.

64. The breach concerns financial data beyond the identity and user ID information, making it particularly severe. The number of individuals affected is high.

65. The fact that a breach could happen in such a sensitive environment points to significant data security holes in the controller's system, and may be an indicator of a time when the review and update of affected measures is "necessary" in line with Articles 24 (1), 25 (1), and 32 (1) of the GDPR. The breached data permits the unique identification of data subjects and contains other information about them (including gender, date and place of birth), furthermore it can be used by the attacker to guess the customers' passwords or to run a spear phishing campaign directed at the bank customers.

66. For these reasons, the data breach was deemed likely to result in a high risk to the rights and freedoms of all the data subjects concerned. Therefore, the occurrence of material (e.g. financial loss) and non-material damage (e.g. identity theft or fraud) is a conceivable outcome.

3.3.2 CASE No. 07 – Mitigation and obligations

67. The controller's measures mentioned in the case description are adequate. In the wake of the breach it also corrected the vulnerability of the website and took other steps to prevent similar future data breaches, such as adding two-factor authentication to the concerned website and moving up to a strong customer authentication.

68. Documenting the breach according to Article 33 (5) GDPR and notifying the SA about it are not optional in this scenario. Furthermore, the controller should notify all 100.000 data subjects (including the data subjects whose accounts were not compromised) in accordance with Article 34 GDPR.

Actions necessary based on the identified risks		
Internal documentation	Notification to SA	Communication to data subjects
✓	✓	✓

3.4 Organizational and technical measures for preventing / mitigating the impacts of hacker attacks

69. Just as in case of ransomware attacks, regardless of the outcome and the consequences of the attack, re-evaluating IT security is compulsory for controllers in similar cases.

70. Advisable measures:[14]

(*The list of the following measures is by no means exclusive or comprehensive. Rather, the goal is to provide prevention ideas and possible solutions. Every processing activity is different, hence the controller should make the decision on which measures fit the given situation the most.*)

- State-of-the-art encryption and key management, especially when passwords, sensitive or financial data are being processed. Cryptographic hashing and salting for secret information (passwords) is always preferred over encryption of passwords. The use of authentication methods obviating the need to process passwords on the server side is preferable.
- Keeping the system up to date (software and firmware). Ensuring that all IT security measures are in place, making sure they are effective and keeping them regularly updated when processing or circumstances change or evolve. In order to be able to demonstrate compliance with Article 5(1)(f) in accordance with Article 5 (2) GDPR the controller should maintain a record of all updates performed, including also the time when they were applied.
- Use of strong authentication methods like two-factor authentication and authentication servers, complemented by an up-to-date password policy.
- Secure development standards include the filtering of user input (using white listing as far as practicable), escaping user inputs and brute force prevention measures (such as limiting the maximum amount of retries). "Web Application Firewalls" may assist in the effective use of this technique.
- Strong user privileges and access control management policy in place.
- Use of appropriate, up-to-date, effective and integrated firewall, intrusion detection and other perimeter defence systems.
- Systematic IT security audits and vulnerability assessments (penetration testing).

[14] For secure web application development see also: https://www.owasp.org/index.php/Main_Page

- Regular reviews and testing to ensure that backups can be used to restore any data whose integrity or availability was affected.
- No session ID in URL in plain text.

4 INTERNAL HUMAN RISK SOURCE

71. The role of human error in personal data breaches has to be highlighted, due to its common appearance. Since these types of breaches can be both intentional and unintentional, it is very hard for the data controllers to identify the vulnerabilities and adopt measures to avoid them. The International Conference of Data Protection and Privacy Commissioners recognized the importance of addressing such human factors and adopted the resolution to address the role of human error in personal data breaches in October 2019[15]. This resolution stresses that appropriate safeguarding measures should be taken to prevent human errors and provides a non-exhaustive list of such safeguards and approaches.

4.1 CASE No. 08: Exfiltration of business data by a former employee

During his period of notice, the employee of a company copies business data from the company's database he is authorized to access, and needs to fulfil his job. Months later, after quitting the job, he uses the data thus gained (mainly basic contact data) to contact the clients of the company to entice them to his new business.

4.1.1 CASE No. 08 - Prior measures and risk assessment

72. In this particular case no prior measures were taken to prevent the employee from copying contact information of the company's clientele, since he needed – and had – legitimate access to this information. Since fulfilling most customer relation jobs require some kind of employee access to personal data, these data breaches may be the most difficult to prevent. Limitations to the scope of access may limit the work the given employee is able to do. However, well thought out access policies and constant control can help prevent such breaches.

73. As usual, during risk assessment the type of the breach and the nature, sensitivity, and volume of personal data affected are to be taken into consideration. These kinds of breaches are typically breaches of confidentiality, since the database is usually left intact, its content "merely" copied for further use. The quantity of data affected is usually also low or medium. In this particular case no special categories of personal data were affected, the employee only needed the contact information of clients to enable him to get in touch with them after leaving the company. Therefore, the data concerned is not sensitive.

74. Although the only goal of the ex-employee that maliciously copied the data may be limited to gaining the contact information of the company's clientele for his own commercial purposes, the controller is not in a position to consider the risk for the affected data subjects to be low, since the controller does not have any kind of reassurance on the intentions of the employee. Thus, while the consequences of the breach might be limited to the exposure to uncalled-for self-marketing of the ex-employee, further and more grave abuse of the stolen data is not ruled out.

[15] The International Conference of Data Protection and Privacy Commissioners, Resolution to address the role of human error in personal data breaches, October 2019, http://globalprivacyassembly.org/wp-content/uploads/2019/10/AOIC-Resolution-FINAL-ADOPTED.pdf

4.1.2 CASE No. 08 – Mitigation and obligations

75. The mitigation of the adverse effects of the breach in the above case is difficult. It might need to involve immediate legal action to prevent the former employee from abusing and disseminating the data any further. As a next step, the avoidance of similar future situations should be the goal. The controller might try to order the ex-employee to stop using the data, but the success of this action is dubious at best.

76. There is no "one-size fits-all" solution to these kinds of cases, but a systematic approach may help to prevent them. For example, the company may consider – when possible - withdrawing certain forms of access from employees who have signalled their intention to quit or implementing access logs so that unwanted access can be logged and flagged. The contract signed with employees should include clauses that prohibit such actions.

77. All in all, as the given breach will not result in a high risk to the rights and freedoms of natural persons, a notification to the SA will suffice. However, the information to the data subjects might be beneficial for the data controller too, since it might be better that they hear from the company about the data leak rather than from the ex-employee who tries to contact them. Data breach documentation in accordance with Article 33 (5) is a legal obligation.

Actions necessary based on the identified risks		
Internal documentation	Notification to SA	Communication to data subjects
✔	✓	x

4.2 CASE No. 09: Accidental transmission of data to a trusted third party

An insurance agent noticed that – made possible by the faulty settings of an Excel file received by e-mail – he was able to access information related to two dozen customers not belonging to his scope. He is bound by professional secrecy and was the sole recipient of the e-mail. The arrangement between the data controller and the insurance agent obliges the agent to signal a personal data breach without undue delay to the data controller. Therefore, the agent instantly signalled the mistake to the controller, who corrected the file and sent it out again, asking the agent to delete the former message. According to the above-mentioned arrangement the agent has to confirm the deletion in a written statement, which he did. The information gained includes no special categories of personal data, only contact data and data about the insurance itself (insurance type, amount). After analysing the personal data affected by the breach the data controller did not identify any special characteristics on the side of the individuals or the data controller that may affect the level of impact of the breach.

4.2.1 CASE No. 09 – Prior measures and risk assessment

78. Unlike the previous case, here the breach does not derive from a deliberate action of an employee, but from an unintentional human error caused by inattentiveness. These kinds of breaches may be avoided by a) enforcing training, education and awareness programs where employees gain a better understanding of the importance of personal data protection, b) reducing file exchange through e-mail, instead using dedicated systems for processing customer data for example, c) double checking files before sending, d) separating the creation and sending of files.

79. This data breach concerns only the confidentiality of the data, and the integrity and the accessibility thereof are left intact. The data breach only concerned about two dozen costumers, hence the quantity of data affected can be considered as low. Furthermore, the personal data affected does not contain any sensitive data. The fact that the data processor immediately contacted the data controller after becoming aware of the data breach can be considered a risk mitigating factor. (The possibility of data having been sent to other insurance agents should also be evaluated and, if confirmed, proper measures should be taken.) Due to the appropriate steps taken after the data breach, it will probably not have any impact on the data subjects' rights and freedoms.

80. The combination of the low number of individuals affected, the immediate detection of the breach and the measures taken to have its effects minimized make this particular case no risk.

4.2.2 CASE No. 09 – Mitigation and obligations

81. Moreover, other risk mitigating circumstances are at play as well: the agent is bound by professional secrecy; he himself reported the problem to the controller; and he deleted the file upon request. Raising awareness and possibly including additional steps in checking documents involving personal data will probably help avoid similar cases in the future.

82. Besides documenting the breach in accordance with Article 33 (5), there is no need for any other action.

Actions necessary based on the identified risks		
Internal documentation	Notification to SA	Communication to data subjects
✓	X	X

4.3 Organizational and technical measures for preventing / mitigating the impacts of internal human risk sources

83. A combination of the below mentioned measures – applied depending on the unique features of the case – should help to lower the chance of a similar breach reoccurring.

84. Advisable measures:

(*The list of the following measures is by no means exclusive or comprehensive. Rather, the goal is to provide prevention ideas and possible solutions. Every processing activity is different, hence the controller should make the decision on which measures fit the given situation the most.*)

- Periodic implementation of training, education and awareness programs for employees on their privacy and security obligations and the detection and reporting of threats to the security of personal data[16]. Develop an awareness program to remind employees of the most commons errors leading to personal data breaches and how to avoid them.

[16] Section 2) subsection (i) of the Resolution to address the role of human error in personal data breaches.

- Establishment of robust and effective data protection and privacy practices, procedures and systems[17].
- Evaluation of privacy practices, procedures and systems to ensure continued effectiveness[18].
- Making proper access control policies and forcing users to follow the rules.
- Implementing techniques to force user authentication when accessing sensitive personal data.
- Disabling the company related account of the user as soon as the person leaves the company.
- Checking unusual dataflow between the file server and employee workstations.
- Setting up I/O interface security in the BIOS or through the use of software controlling the use of computer interfaces (lock or unlock e. g. USB/CD/DVD etc.).
- Reviewing employees' access policy (e.g. logging access to sensitive data and requiring the user to input a business reason, so that this is available for audits).
- Disabling open cloud services.
- Forbidding and preventing access to known open mail services.
- Disabling print screen function in OS.
- Enforcing a clean desk policy.
- Automated locking all computers after a certain amount of time of inactivity.
- Use mechanisms (e.g. (wireless) token to log on/open locked accounts) for fast user switches in shared environments.
- Use of dedicated systems for managing personal data that apply appropriate access control mechanisms and that prevent human mistake, such as sending of communications to the wrong subject. The use of spreadsheets and other office documents is not an appropriate means to manage client data.

5 LOST OR STOLEN DEVICES AND PAPER DOCUMENTS

85. A frequent type of case is the loss or theft of portable devices. In these cases, the controller has to take into consideration the circumstances of the processing operation, such as the type of data stored on the device, as well as the supporting assets, and the measures taken prior to the breach to ensure an appropriate level of security. All of these elements affect the potential impacts of the data breach. The risk assessment might be difficult, as the device is no longer available.

[17] Section 2) subsection (ii) of the Resolution to address the role of human error in personal data breaches.

[18] Section 2) subsection (iii) of the Resolution to address the role of human error in personal data breaches.

86. These kinds of breaches can be always classified as breaches of confidentiality. However, if there is no backup for the stolen database, then the breach type can also be breach of availability and breach of integrity.

87. The scenarios bellow demonstrate how the above mentioned circumstances influence the likelihood and severity of the data breach.

5.1 CASE No. 10: Stolen material storing encrypted personal data

During a break-in into a children's day-care centre, two tablets were stolen. The tablets contained an app which held personal data about the children attending the day-care centre. Name, date of birth, personal data about the education of the children were concerned. Both the encrypted tablets which were turned off at the time of the break-in, and the app were protected by a strong password. Back-up data was effectively and readily available to the controller. After becoming aware of the break-in, the day-care remotely issued a command to wipe the tablets shortly after the discovery of the break-in.

5.1.1 CASE No. 10 - Prior measures and risk assessment

88. In this particular case the data controller took adequate measures to prevent and mitigate the impacts of a potential data breach by using device encryption, introducing adequate password protection and securing back-up of the data stored on the tablets. (A list of advisable measures is to be found in section 5.7).

89. After becoming aware of a breach, the data controller should assess the risk source, the systems supporting the data processing, the type of personal data involved and the potential impacts of the data breach on the concerned individuals. The data breach described above would have concerned confidentiality, availability and integrity of the concerned data, however due to the appropriate proceedings of the data controller prior and after the data breach none of these occurred.

5.1.2 CASE No. 10 – Mitigation and obligations

90. The confidentiality of the personal data on the devices was not compromised due to the strong password protection on both the tablets and the apps. The tablets were set up in such a way that setting a password also means that the data on the device is encrypted. This was further enhanced by the controller's action to attempt to remotely wipe everything from the stolen devices.

91. Due to the measures taken, the confidentiality of the data was kept intact too. Furthermore, the backup ensured the continuous availability of the personal data, hence no potential negative impact could have occurred.

92. Due to these facts, the above described data breach was unlikely to result in a risk to the rights and freedoms of the data subjects, hence no notification to the SA or the concerned data subjects was necessary. However, this data breach must also be documented in accordance with Article 33 (5).

Actions necessary based on the identified risks		
Internal documentation	Notification to SA	Communication to data subjects
✓	X	X

5.2 CASE No. 11: Stolen material storing non-encrypted personal data

The electronic notebook device of an employee of a service provider company was stolen. The stolen notebook contained names, surnames, sex, addresses and date of births of more than 100000 customers. Due to the unavailability of the stolen device it was not possible to identify if other categories of personal data were also affected. The access to the notebook's hard drive was not protected by any password. Personal data could be restored from daily backups available.

5.2.1 CASE No. 11 - Prior measures and risk assessment

93. No prior safety measures were taken by the data controller, hence the personal data stored on the stolen notebook was easily accessible for the thief or any other person coming into possession of the device thereafter.

94. This data breach concerns the confidentiality of the data stored on the stolen device.

95. The notebook containing the personal data was vulnerable in this case because it did not possess any password protection or encryption. The lack of basic security measures enhances the risk level for the affected data subjects. Furthermore, the identification of the concerned data subjects is also problematic, which also increases the severity of the breach. The considerable number of concerned individuals increases the risk, nevertheless, no special categories of personal data were concerned in the data breach.

96. During the risk assessment the controller should take into consideration the potential consequences and adverse effects of the confidentiality breach. As a result of the breach the concerned data subjects may suffer identity fraud relying on the data available on the stolen device, so risk is considered to be high.

5.2.2 CASE No. 11 – Mitigation and obligations

97. Turning on device encryption and the use of strong password protection of the stored database could have prevented the data breach to result in a risk to the rights and freedoms of the data subjects.

98. Due to these circumstances the notification of the SA is required, the notification of the concerned data subjects is also necessary.

Actions necessary based on the identified risks		
Internal documentation	Notification to SA	Communication to data subjects
✓	✓	✓

5.3 CASE No. 12: Stolen paper files with sensitive data

A paper log book was stolen from a drug addiction rehab facility. The book contained basic identity and health data of the patients admitted to the rehab facility. The data was only stored on paper and no backup was available to the doctors treating the patients. The book was not stored in a locked drawer or a room, the data controller had neither an access control regime nor any other safeguarding measure for the paper documentation.

5.3.1 CASE No. 12 – Prior measures and risk assessment

99. No prior safety measures were taken by the data controller, hence the personal data stored in this book was easily accessible for the person who found it. Moreover, the nature of the personal data stored in the book makes the lack of backup data a very serious risk factor.

100. This case serves as an example for a high-risk data breach. Due to the failure of appropriate safety precautions, sensitive health data pursuant to Article 9 (1) GDPR was lost. Since in this case a special category of personal data was concerned, the potential risks to the concerned data subjects was increased, which should be also taken into consideration by the controller assessing the risk.

101. This breach concerns the confidentiality, availability and integrity of the concerned personal data. As a result of the breach, medical secrecy is broken and unauthorized third parties may gain access to the patients' private medical information, what may have severe impact on the patient's personal life. The availability breach may also disturb the continuity of the patients' treatment. Since the modification/deletion of parts of the book's content may not be excluded, the integrity of the personal data is also compromised.

5.3.2 CASE No. 12 – Mitigation and obligations

102. During the assessment of the safeguarding measures the type of the supporting asset should be considered as well. Since the patient log book was a physical document, its safeguarding should have been organized differently than that of an electronic device. The pseudonymisation of the patients' names, the storage of the book in a safeguarded premises and in a locked drawer or a room, and proper access control with authentication when accessing it could have prevented the data breach.

103. The above described data breach may severely impact the concerned data subjects; hence the notification of the SA and communication of the breach to the concerned data subjects is mandatory.

Actions necessary based on the identified risks		
Internal documentation	Notification to SA	ommunication to data subjects
✔	✓	✓

5.4 Organizational and technical measures for preventing / mitigating the impacts of loss or theft of devices

104. A combination of the below mentioned measures – applied depending on the unique features of the case – should help to lower the chance of a similar breach reoccurring.

105. Advisable measures:

(*The list of the following measures is by no means exclusive or comprehensive. Rather, the goal is to provide prevention ideas and possible solutions. Every processing activity is different, hence the controller should make the decision on which measures fit the given situation the most.*)

- Turn on device's encryption (such as Bitlocker, Veracrypt or DM-Crypt).
- Use passcode/password on all devices. Encrypt all mobile electronic devices in a way that requires the input of a complex password for decryption.
- Use multi-factor authentication.
- Turn on the functionalities of highly mobile devices that allow them to be located in case of loss or misplacement.
- Use MDM (Mobile Devices Management) software/app and localization. Use anti-glare filters. Close down any unattended devices.

- If possible and appropriate to the data processing in question, save personal data not on a mobile device, but on a central back-end server.
- If the workstation is connected to the corporate LAN, do an automatic backup from the work folders provided it is unavoidable that personal data is stored there
- Use a secure VPN (e.g. which requires a separate second factor authentication key for the establishment of a secure connection) to connect mobile devices to back-end servers.
- Provide physical locks to employees in order to enable them to physically secure mobile devices they use while they remain unattended.
- Proper regulation of device usage outside the company.
- Proper regulation of device usage inside the company.
- Use MDM (Mobile Devices Management) software/app and enable the remote wipe function.
- Use centralised device management with minimum rights for the end users to install software.
- Install physical access controls.
- Avoid storing sensitive information in mobile devices or hard drives. If there is need to access the company's internal system, secure channels should be used such as previously stated.

6 MISPOSTAL

106. The risk source is an internal human error in this case as well, but here no malicious action led to the breach. It is the result of inattentiveness. Little can be undertaken by the controller after it happened, so prevention is even more important in these cases than in other breach types.

6.1 CASE No. 13: Snail mail mistake

Two orders for shoes were packed by a retail company. Due to human error two packing bills were mixed up with the result that both products and the relevant packing bills were sent to the wrong person. This means that the two customers got each other's orders, including the packing bills containing the personal data. After becoming aware of the breach the data controller recalled the orders and sent them to the right recipients.

6.1.1 CASE No. 13 - Prior measures and risk assessment

107. The bills contained the personal data required for a successful delivery (name, address, plus the item purchased and its price). It is important to identify how the human error could have happened in the first place, and if in any way, it could have been prevented. In the particular case describe the risk is low, since no special categories of personal data or other data whose abuse might lead to substantial negative effects were involved, the breach is not a result of a systemic error on the controller's part and only two individuals are concerned. No negative effect on the individuals could be identified.

6.1.2 CASE No. 13 – Mitigation and obligations

108. The controller should provide for a free return of the items and the accompanying bills, and it also should request the wrong recipients to destroy / delete all eventual copies of the bills containing the other person's personal data.

109. Even if the breach itself does not pose a high risk to rights and freedoms of the affected individuals, and thus communication to the data subjects is not mandated by Article 34 GDPR, communication of the breach to them cannot be avoided, as their cooperation is needed to mitigate the risk.

Actions necessary based on the identified risks		
Internal documentation	Notification to SA	Communication to data subjects
✓	X	X

6.2 CASE No. 14: Sensitive personal data sent by mail by mistake

The employment department of a public administration office sent an e-mail message – about upcoming trainings - to the individuals registered in its system as jobseekers. By mistake, a document containing all these jobseekers' personal data (name, e-mail address, postal address, social security number) was attached to this e-mail. The number of affected individuals is more than 60000. Subsequently the office contacted all the recipients and asked them to delete the previous message and not to use the information contained in it.

6.2.1 CASE No. 14 - Prior measures and risk assessment

110. Stricter rules should have been implemented for sending such messages. The introduction of additional control mechanisms need to be considered.

111. The number of affected individuals is considerable, and the involvement of their social security number, along with other, more basic personal data, further increases the risk, which can be identified as high. The eventual distribution of the data by any of the recipients cannot be contained by the controller.

6.2.2 CASE No. 14 – Mitigation and obligations

112. As mentioned earlier, the means to effectively mitigate the risks of a similar breach, are limited. Though the controller asked for the deletion of the message, it cannot force the recipients to do so, and as a consequence, nor can it be certain that they comply with the request.

113. The execution of all three below indicated actions should be self-evident in a case like this.

Actions necessary based on the identified risks		
Internal documentation	Notification to SA	Communication to data subjects
✓	✓	✓

6.3 CASE No. 15: Personal data sent by mail by mistake

A list of participants on a course in Legal English which takes place in a hotel for 5 days is by mistake sent to 15 former participants of the course instead of the hotel. The list contains names, e-mail addresses and food preferences of the 15 participants. Only two participants have filled in their food preferences, stating that they are lactose intolerant. None of the participants have a protected identity. The controller discovers the mistake immediately after sending the list and informs the recipients of the mistake and asks them to delete the list.

6.3.1 CASE No. 15 - Prior measures and risk assessment

114. Stricter rules should have been implemented for sending of such messages. The introduction of additional control mechanisms need to be considered.

115. The risks deriving from the nature, the sensitivity, the volume and the context of the personal data are low. The personal data includes sensitive data on food preferences of two of the participants. Even if the information that someone is lactose intolerant is health data, the risk that this data will be used in a detrimental way should be considered relatively low. While in the case of data concerning health it is usually assumed that the breach is likely to result in a high risk for the data subject[19], at the same time in this particular case no risk can be identified that the breach will lead to physical, material or non-material damages of the data subject due to the unauthorised disclosure of lactose intolerance information. Contrary to some other food preferences, lactose intolerance can normally not be linked to any religious or philosophical beliefs. The quantity of the breached data and the number of affected data subjects is very low as well.

6.3.2 CASE No. 15 – Mitigation and obligations

116. In summary, it can be stated that the breach had no significant effect on the data subjects. The fact that the controller immediately contacted the recipients after becoming aware of the mistake can be considered as a mitigating factor.

117. If an email is sent to an incorrect/unauthorised recipient, it is recommended that the data controller should Bcc a follow up email to the unintended recipients apologising, instructing that the offending email should be deleted, and advising recipients that they do not have the right to further use the email addresses identified to them.

118. Due to these facts this data breach was unlikely to result in a risk to the rights and freedoms of the data subjects, hence no notification to the SA or the concerned data subjects was necessary. However, this data breach must also be documented in accordance with Article 33 (5).

Actions necessary based on the identified risks		
Internal documentation	Notification to SA	Communication to data subjects
✓	X	X

6.4 CASE No. 16: Snail mail mistake

An insurance group offers car insurances. To do this, it sends out regularly adjusted contribution policies by snail mail. In addition to the name and address of the policyholder, the letter contains the vehicle registration number, the insurance rates of the current and next insurance year, the approximate annual mileage and the policyholder's date of birth. Health data according to Article 9 GDPR, payment data (bank details), economic and financial data are not included.

Letters are packed by automated enveloping machines. Due to a mechanical error, two letters for different policyholders are inserted into one envelope and sent to one policyholder by letter post. The policyholder opens the letter at home and takes a look at his correctly delivered letter as well as at the incorrectly delivered letter from another policyholder.

[19] See Guidelines WP 250, p. 23.

6.4.1 CASE No. 16 - Prior measures and risk assessment

119. The incorrectly delivered letter contains the name, address, date of birth, license plate number and the classification of the insurance rate of the current and the next year. If the insurance rate increases in the following year, this indicates a motor vehicle claim submitted to the insurance company. The effects on the affected person are to be regarded as medium, since information not publicly available such as the date of birth or vehicle registration numbers, and if the insurance rate increases, a not insignificant claim, which could also have been an accident, was disclosed to the unauthorized recipient. The probability of misuse of this data is assessed to be between low and medium. However, while many recipients will probably dispose of the wrongly received letter in the garbage, in individual cases it cannot be completely ruled out that the letter will be posted in social networks or that the policyholder will be contacted.

6.4.2 CASE No. 16 – Mitigation and obligations

120. The controller should have the original document returned at its own expense. The wrong recipient should also be informed that he/she may not misuse the information read.

121. It will probably never be possible to completely prevent a postal delivery error in a mass mailing using fully automated machines. However, in the event of an increased frequency, it is necessary to check whether the enveloping machines are set and maintained correctly enough, or if some other systemic issue leads to such a breach.

Actions necessary based on the identified risks		
Internal documentation	Notification to SA	Communication to data subjects
✓	✓	X

6.5 Organizational and technical measures for preventing / mitigating the impacts of mispostal

122. A combination of the below mentioned measures – applied depending on the unique features of the case - should help to lower the chance of a similar breach reoccurring.

123. Advisable measures:

(*The list of the following measures is by no means exclusive or comprehensive. Rather, the goal is to provide prevention ideas and possible solutions. Every processing activity is different, hence the controller should make the decision on which measures fit the given situation the most.*)

- Setting exact standards – with no room for interpretation - for sending letters / e-mails.
- Adequate training for personnel on how to send letters / e-mails.
- When sending e-mails to multiple recipients, they are listed in the 'bcc' field by default.
- Extra confirmation is required when sending e-mails to multiple recipients, and they are not listed in the 'bcc' field.
- Application of the four-eyes principle.
- Automatic addressing instead of manual, with data extracted from an available and up-to-date database; the automatic addressing system should be regularly reviewed to check for hidden errors and incorrect settings.

- Application of message delay (e.g. the message can be deleted / edited within a certain time period after clicking the press button).
- Disabling autocomplete when typing in e-mail addresses.
- Awareness sessions on most common mistakes leading to a personal data breach.
- Training sessions and manuals on how to handle incidents leading to a personal data breach and who to inform (involve DPO).

7 OTHER CASES – SOCIAL ENGINEERING

7.1 CASE No. 17: Identity theft

The contact centre of a telecommunication company receives a telephone call from someone that poses as a client. The supposed client demands the company to change the email address to which the billing information should be sent from there on. The worker of the contact centre validates the client's identity by asking for certain personal data, as defined by the procedures of the company. The caller correctly indicates the requested client's fiscal number and postal address (because he had access to these elements). After the validation, the operator makes the requested change and, from there on, the billing information is sent to the new email address. The procedure does not foresee any notification to the former email contact. The following month the legitimate client contacts the company, inquiring why he is not receiving billing to his email address, and denies any call from him demanding the change of the email contact. Later, the company realizes that the information has been sent to an illegitimate user and reverts the change.

7.1.1 CASE No. 17 - Risk assessment, mitigation and obligations

124. This case serves as an example on the importance of prior measures. The breach, from a risk aspect, presents a high level of risk, as billing data can give information about the data subject's private life (e.g. habits, contacts) and could lead to material damage (e.g. stalking, risk to physical integrity). The personal data obtained during this attack can also be used in order to facilitate account takeover in this organisation or exploit further authentication measures in other organisations. Considering these risks, the "appropriate" authentication measure should meet a high bar, depending on what personal data can be processed as a result of authentication.

125. As a result, both a notification to the SA and a communication to the data subject are needed from the controller.

126. The prior client validation process is clearly to be refined in light of this case. The methods used for authentication were not sufficient. The malicious party was able to pretend to be the intended user by the use of publicly available information and information that they otherwise had access to.

127. The use of this type of static knowledge-based authentication (where the answer does not change, and where the information is not "secret" such as would be the case with a password) is not recommended.

128. Instead, the organisation should use a form of authentication which would result in a high degree of confidence that the authenticated user is the intended person, and not anyone else. The introduction of an out-of-band multi-factor authentication method would solve the problem, e.g. to verify the change demand, by sending a confirmation request to the former contact; or adding extra questions and requiring

information only visible on the previous bills. It is the controller's responsibility to decide which measures to introduce, as it knows the details and requirements of its internal operation the best.

Actions necessary based on the identified risks		
Internal documentation	Notification to SA	Communication to data subjects
✓	✓	✓

7.2 CASE No. 18: Email exfiltration

A hypermarket chain detected, 3 months after its configuration, that some email accounts had been altered and rules created so that every email containing certain expressions (e.g. "invoice", "payment", "bank wiring", "credit card authentication", "bank account details") would be moved to an unused folder and also forwarded to an external email address. Also, by that time, a social engineering attack had already been performed, i.e., the attacker, posing as a supplier, had had that supplier bank account details altered into his own. Finally, by that time, several fake invoices had been sent that included the new bank account detail. The monitoring system of the email platform ended up giving an alert regarding the folders. The company was unable to detect how the attacker was able to gain access to the email accounts to begin with, but it supposed that an infected email was to blame for giving access to the group of users in charge of the payments.

Due to the keyword-based forwarding of emails, the attacker received information on 99 employees: name and wage of a particular month regarding 89 data subjects; name, civil status, number of children, wage, work hours and remainder information on the salary receipt of 10 employees whose contracts were ended. The controller only notified the 10 employees belonging to the latter group.

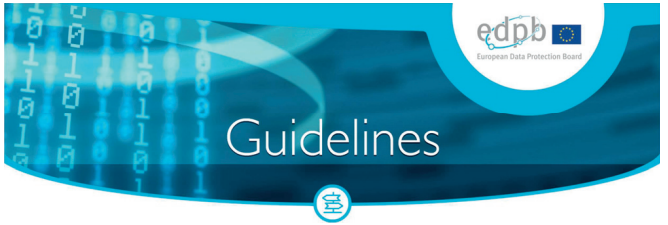
7.2.1 CASE No. 18 - Risk assessment, mitigation and obligations

129. Even if the attacker was probably not aiming at collecting personal data, since the breach could lead to both material (e.g. financial loss) and non-material damage (e.g. identity theft or fraud), or the data could be used to facilitate other attacks (e.g. phishing), the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons. Therefore the breach should be communicated to all 99 employees and not only to the 10 employees whose salary information was leaked.

130. After becoming aware of the breach, the controller forced a password change for the compromised accounts, blocked sending emails to the attacker's email account, notified the service provider of the email used by the attacker regarding his or her actions, removed the rules set by the attacker and refined the alerts of the monitoring system in order to give an alert as soon as an automatic rule is created. Alternatively, the controller could remove the right for users to set forwarding rules, needing the IT service team to do it only on request or it could introduce a policy that users should check and report on the rules set on their accounts once per week or more often, in areas handling financial data.

131. The fact that a breach could happen and go undetected for so long and the fact that, in a longer time, social engineering could have been used for altering more data, highlighted significant problems in the controller's IT security system. These should be addressed without delay, like emphasizing automation reviews and change controls, incident detection and response measures. Controllers handling sensitive data, financial information, etc. have a larger responsibility in terms of providing adequate data security.

Actions necessary based on the identified risks		
Internal documentation	Notification to SA	Communication to data subjects
✓	✓	✓



Guidelines 10/2020 on restrictions under Article 23 GDPR

Version 2.0

Adopted on 13 October 2021

Version Table

Version 1.0	15 December 2020	Adoption of the Guidelines for public consultation
Version 2.0	13 October 2021	Adoption of the Guidelines after public consultation

Table of contents

1 Introduction 5

2 The meaning of restrictions 6

3 Requirements of Article 23(1) GDPR 7

3.1 Respect of the essence of the fundamental rights and freedoms 7

3.2 Legislative measures laying down restrictions and the need to be foreseeable (Recital 41 and CJEU case law) 7

3.3 Grounds for the restrictions 9

3.3.1 National security, defence and public security 9

3.3.2 Prevention, investigation, detection and prosecution of criminal offences or the execution of criminal penalties including the safeguarding against and the prevention of threats to public security 9

3.3.3 Other important objectives of general public interest 9

3.3.4 Protection of judicial independence and judicial proceedings 10

3.3.5 Prevention, investigation, detection and prosecution of breaches of ethics for regulated professions 10

3.3.6 Monitoring, inspection or regulatory function connected to the exercise of official authority in the cases referred to in points (a) to (e) and (g) of Article 23 GDPR 10

3.3.7 Protection of the data subject or the rights and freedoms of others 11

3.3.8 Enforcement of civil law claims 11

3.4 Data subjects' rights and controller's obligations which may be restricted 11

3.5 Necessity and proportionality test 11

4 Requirements of Article 23(2) GDPR 13

4.1 Categories of personal data 13

4.2 Scope of the restrictions 14

4.3 Safeguards to prevent abuse or unlawful access or transfer 14

4.4 Specification of the controller 14

4.5 Storage periods 14

4.6 Risks to data subjects' rights and freedoms 14

4.7 Right to be informed about the restriction, unless prejudicial to the purpose of the restriction 15

5 Consultation with the SAs (Articles 36(4) and 57(1)(c) GDPR) 16

6 Non - observation of article 23 GDPR requirements by a Member State 16

7 Specific elements for controllers and processors 16

7.1 Accountability Principle 16

7.2 Exercise of data subject's rights after the lifting of the restriction 17

7.3 Non-observation of a legislative measure imposing such restrictions by a controller 17

8 Conclusions 18

9 Annex: Check-lists - Article 23 GDPR in a nutshell 19

9.1 Requirements under Article 23(1) GDPR 19

9.2 Requirements under Article 23(2) GDPR 19

The European Data Protection Board

Having regard to Article 70 (1)(e) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, (hereinafter 'GDPR'),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018[1],

Having regard to Article 12 and Article 22 of its Rules of Procedure,

HAS ADOPTED THE FOLLOWING GUIDELINES

1 INTRODUCTION

1. This document seeks to provide guidance as to the application of Article 23 GDPR. These Guidelines provide a thorough analysis of the criteria to apply restrictions, the assessments that need to be observed, how data subjects can exercise their rights once the restriction is lifted and the consequences for infringements of Article 23 GDPR.

2. The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 16(2) of the Treaty on the Functioning of the European Union mandates the European Parliament and the Council to lay down the rules in relation to the protection of personal data and the rules relating to the free movement of personal data. The GDPR protects the rights and freedoms of natural persons and in particular their right to data protection. Data protection cannot be ensured without adhering to the rights and principles set out in the GDPR (Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided in Articles 12 to 22 GDPR). All these rights and obligations are at the core of the fundamental right to data protection and their application should be the general rule. In particular, any limitation to the fundamental right to data protection needs to observe Article 52 of the Charter of fundamental rights of the European Union ('the Charter').

3. It is against this background that Article 23 GDPR should be read and interpreted. This provision is entitled 'restrictions'. It provides that, under Union or Member State law, the application of certain provisions of the Regulation, relating to the rights of the data subjects and controllers' obligations, may be restricted in the situations therein listed. Restrictions should be seen as exceptions to the general rule allowing the exercise of rights and imposing the obligations enshrined in the GDPR[2]. As such, restrictions should be interpreted narrowly, only be applied in specifically provided circumstances and only when certain conditions are met.

4. Even in exceptional situations, the protection of personal data cannot be restricted in its entirety. It must be upheld in all emergency measures, as per Article 23 GDPR thus contributing to the respect of the overarching values of democracy, rule of law and fundamental rights on which the Union is founded: any measure taken by Member States shall respect the general principles of law, the essence of the fundamental rights and freedoms and shall not be irreversible and data controllers and processors shall continue to comply with data protection rules.

5. In all cases, where Union or Member State law allows restrictions to data subjects' rights or to the obligations of the controllers (including joint controllers[3]) and processors[4], it should be noted that the accountability principle, as laid down in Article 5(2) GDPR, is still applicable. This means that the controller is responsible for, and shall be able to demonstrate to the data subjects his or her compliance with the EU data protection framework, including the principles relating to the processing of their data.

6. When the EU or national legislator lays down restrictions based on Article 23 GDPR, it shall ensure that it meets the requirements set out in Article 52(1) of the Charter, and in particular conduct a proportionality assessment so that restrictions are limited to what is strictly necessary.

2 THE MEANING OF RESTRICTIONS

7. The term restrictions is not defined in the GDPR. Article 23 and Recital 73 GDPR only list the conditions under which restrictions can be applied.

8. In these guidelines, the term restrictions will be defined as any limitation of scope of the obligations and rights provided for in Articles 12 to 22 and 34 GDPR as well as corresponding provisions of Article 5 in accordance with Article 23 GDPR. A restriction to an individual right has to safeguard important objectives, for instance, the protection of rights and freedoms of others or important objectives of general public interest of the Union or of a Member State which are listed in Article 23(1) GDPR. Therefore, restrictions of data subjects' rights can only occur when the listed interests are at stake[5] and these restrictions aim at safeguarding such interests.

9. Consequently, the grounds for the restriction need to be clear. To be lawful, restrictions shall be provided for in a legislative measure, concern a limited number of rights of data subjects and/or controller's obligations which are listed in Article 23 GDPR[6], respect the essence of the fundamental rights and freedoms at issue, be a necessary and proportionate measure in a democratic society and safeguard one of the grounds set out in Article 23(1) GDPR as described below.

[1] References to 'Member States' made throughout this document should be understood as references to 'EEA Member States'.
[2] These situations do not include the scenarios where the Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA applies.
[3] In case of joint controllership, especially in case where controllers are from different Member States, restrictions applicable in accordance with Article 23 should be considered and taken into account so that joint controllers clarify in the arrangement their respective roles.
[4] Although from now on the guidelines will refer to 'controllers' only, the recommendations are addressed, where applicable, also to processors.
[5] These interests are exhaustively listed in Article 23(1) GDPR.
[6] There are certain rights which cannot be restricted under Article 23 GDPR, such as the right to submit a complaint to the supervisory authority (Article 77 GDPR).

10. Furthermore, as mentioned in Recital 73 GDPR, restrictions should be in accordance with the requirements set out in the Charter and the European Convention for the Protection of Human Rights and Fundamental Freedoms.

11. In addition to restrictions referred to in Article 23, the GDPR also lays down provision relating to specific processing situations as per Chapter IX, where Member States may provide by law specific measures impacting data subjects' rights, such as exemptions or derogations (for instance, Articles 85 or 89 GDPR). However these guidelines do not address those cases.

12. Restricting the scope of the obligations and rights provided for in Article 12 to 22 and Article 34 may take different forms but may never reach the point of a general suspension of all rights. Legislative measures laying down restrictions under Article 23 GDPR may also foresee that the exercise of a right is delayed in time, that a right is exercised partially or circumscribed to certain categories of data or that a right can be exercised indirectly through an independent supervisory authority.

3 REQUIREMENTS OF ARTICLE 23(1) GDPR

13. Article 23(1) GDPR lists a number of requirements, which are detailed below. All those requirements need to be met in order for a measure to be lawfully relied upon.

3.1 Respect of the essence of the fundamental rights and freedoms

14. One of the main objectives of data protection law is to enhance data subjects' control over personal data concerning them. Any restriction shall respect the essence of the right that is being restricted. This means that restrictions that are extensive and intrusive to the extent that they void a fundamental right of its basic content, cannot be justified. In any case, a general exclusion of data subjects' rights with regard to all or specific data processing operations or with regard to specific controllers would not respect the essence of the fundamental right to the protection of personal data, as enshrined in the Charter. If the essence of the right is compromised, the restriction shall be considered unlawful, without the need to further assess whether it serves an objective of general interest or satisfies the necessity and proportionality criteria.

15. In order to guarantee this control, data subjects have a number of rights within the right to data protection and the controller has a number of obligations vis a vis the data subject, set out under Articles 12 to 22 and Article 34 GDPR, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22 GDPR. It is against this background that Article 23 GDPR should be read and interpreted.

3.2 Legislative measures laying down restrictions and the need to be foreseeable (Recital 41 and CJEU case law)

16. The requirement of a legislative measure entails that controllers can only rely on a restriction provided for by Article 23 GDPR to the extent that this restriction has been specified in Union or Member state law. Without the corresponding legislative measure, controllers cannot rely directly on the grounds listed in Article 23(1) GDPR. Recital 41 GDPR states that '[w]here this Regulation refers to a legal basis or a legislative measure, this does not necessarily require a legislative act adopted by a parliament, without prejudice to requirements pursuant to the constitutional order of the Member State concerned. However, such a legal basis or legislative measure should be clear and precise and its application should be foreseeable to persons subject to it, in accordance with the case-law of the Court of Justice of the European Union [...] and the European Court of Human Rights'[7].

17. According to Article 52(1) of the Charter, any limitation on the exercise of the rights and freedoms recognised by the Charter shall be 'provided for by law'. This echoes the expression 'in accordance with the law' in Article 8(2) of the European Convention of Human Rights[8], which means not only compliance with domestic law, but also relates to the quality of that law without prejudice to the nature of the act, requiring it to be compatible with the rule of law. In particular, the domestic law must be **sufficiently clear in its terms to give individuals an adequate indication of the circumstances in and conditions under which controllers are empowered to resort to any such restrictions**. The same strict standard should be applied for any restrictions that could be imposed by Member States. In line with the GDPR and the case law of the Court of Justice of the European Union (CJEU) and of the European Court of Human Rights (ECtHR), it is indeed essential that legislative measures, which seek to restrict the scope of data subject rights or of controller's obligations, are foreseeable for the data subjects.

18. While any legislative measure must in any case be adapted to the objective pursued and meet the foreseeability criterion, a legislative measure laying down the provisions for the application of restrictions under Article 23 GDPR does not always have to be limited in time or linked to a specific period.

    a. In some cases, the restriction is not specifically linked to a timeframe because the ground for the restriction to be safeguarded by the legislative measure is not in itself limited in time. In light of the principle of necessity and proportionality, it is necessary to ensure that such legislative measures relate to a ground for restriction to be safeguarded on an ongoing basis, or permanently, in a democratic society. For instance, a legislative measure restricting the scope of the obligations and rights provided for in Article 12 to 22 and Article 34, for safeguarding the protection of judicial independence and judicial proceedings may for example be considered as fulfilling a continuing objective in a democratic society and therefore may not be limited in time.

    b. In other cases, the ground for the restriction to be safeguarded is in itself limited in time and therefore the legislative measure should provide a limitation in time in order to meet the foreseeability criterion. For example, where restrictions are adopted in the context of a state of emergency to safeguard public health, the EDPB considers that restrictions, imposed for a duration not precisely limited in time, do not meet the foreseeability

[7] The type of legislative measures considered has to be in line with EU law or with the national law. Depending on the degree of interference of the restriction, a particular legislative measure, taking into account the level of norm, could be required at national level.

[8] See in particular, European Court of Human Rights, 14 September 2010, Sanoma Uitgevers B.V. v. The Netherlands, EC:ECHR:2010:0914JUD003822403, paragraph 83: 'Further, as regards the words "in accordance with the law" and "prescribed by law" which appear in Articles 8 to 11 of the Convention, the Court observes that it has always understood the term "law" in its "substantive" sense, not its "formal" one; it has included both "written law", encompassing enactments of lower ranking statutes and regulatory measures taken by professional regulatory bodies under independent rule-making powers delegated to them by Parliament, and unwritten law. "Law" must be understood to include both statutory law and judge-made "law". In sum, the "law" is the provision in force as the competent courts have interpreted it'. On the notion of 'provided for by law', the criteria developed by the European Court of Human Rights should be used as suggested in CJEU Advocate General opinions in joined cases C‑203/15 and C‑698/15, Tele2 Sverige AB, ECLI:EU:C:2016:572, paragraphs 137-154 or in case C-70/10, Scarlet Extended, ECLI:EU:C:2011:255, paragraph 99.

criterion, including when such restriction apply retroactively or are subject to undefined conditions[9].

19. This link between the foreseen restrictions and the objective pursued should be clearly established and demonstrated in the concerned legislative measure or additional supplementary documents. For instance, the mere existence of a pandemic alone is not a sufficient reason to provide for any kind of restriction on the rights of data subjects; rather, any restriction shall clearly contribute to the safeguard of an important objective of general public interest of the Union or of a Member State.

3.3 Grounds for the restrictions

20. In order to adopt a legislative measure for restrictions and to apply a restriction in a concrete case, one or several of the following conditions stated in Article 23(1) GDPR need to be met. This list is exhaustive, meaning restrictions cannot be carried out under any other conditions than the ones listed below.

21. The link between the foreseen restrictions and the objective pursued should be clearly stated in the legislative measure.

3.3.1 National security, defence and public security

22. A restriction to data subject rights can have national or public security and/or defence of the Member States as an objective to be safeguarded, as stated in Article 23(1)(a), (b) and (c) GDPR.

23. Moreover, public security includes protection of human life, especially in response to natural or manmade disasters.

3.3.2 Prevention, investigation, detection and prosecution of criminal offences or the execution of criminal penalties including the safeguarding against and the prevention of threats to public security

24. In certain cases, providing information to the data subjects who are under investigation might jeopardise the success of that investigation. Therefore, the restriction of the right to information or other data subject's rights may be necessary, under Article 23(1)(d) GDPR. This is relevant for instance in the framework of anti-money laundering or the activities of forensic laboratories[10].

25. Nonetheless, the omitted information shall, in accordance with the case law of the CJEU, be provided once and if it is no longer possible for it to jeopardise the investigation being carried out[11]. This means that a specific (tailor-made) data protection notice should be given to the data subject as soon as possible, stating the different rights such as access, rectification etc.

26. Also, the objective of safeguarding public security includes the protection of human life especially in response to natural or manmade disasters[12].

3.3.3 Other important objectives of general public interest

27. Article 23(1)(e) GDPR mentions as other important objectives of general public interest of the Union or of a Member State important economic or financial interest, including monetary, budgetary and taxation matters, public health and social security. It may concern for instance the keeping of public registers kept for reasons of general public interest or the further processing of archived personal data to provide specific information related to the political behaviour under former totalitarian state regimes[13]. However, the costs incurred as a consequence of providing information and thus the financial burden on public budgets are not sufficient to justify a public interest in restricting the rights of the data subjects. As an example a Direct Tax Administration may impose restrictions to the rights of access by the data subject where he or she is under an investigation led by the Tax Administration in the framework of its legal duty, in so far as this access would jeopardise the ongoing investigation. However such restriction should be limited to the time necessary for the specific investigation and should be lifted as soon as the Tax Administration closes the investigation. The data subject should be informed without delay and be notified with the justifications contained in the decision of the controller and with the date from which he or she may again exercise his or her right of access. Also appropriate safeguards should be ensured such as for instance an indirect access[14] - when it is foreseen in national law - so as to ensure that an independent Authority may check the lawfulness of the processing.

28. In order to ensure the general public interest objective of accessibility of the law, a public administration may impose restrictions to the right to object the processing of pseudonymised personal data for the development of a benchmark document and information identifying, by type of damage, the amounts claimed and offered by the parties to a dispute as well as the amounts allocated to victims as compensation for their physical injury in court decisions delivered on appeal by administrative courts and civil courts. Such restrictions may take place provided that the conditions under Article 23(2) GDPR are met, and in particular through the implementation of safeguards such as the approximation of compensation amounts, the deletion of the first and last names of the parties to the dispute and the pseudonymisation of the personal data processed.

3.3.4 Protection of judicial independence and judicial proceedings

29. Article 23(1)(f) GDPR also foresees the need to restrict certain data subjects' rights or controller's obligations, in order to protect judicial independence and judicial proceedings.

30. The scope of these restrictions should be aligned with national legislation regulating these matters.

3.3.5 Prevention, investigation, detection and prosecution of breaches of ethics for regulated professions

31. Article 23(1)(g) GDPR mentions breaches of ethics for regulated professions, such as medical doctors and lawyers.

32. These are cases in which an investigation does not relate in principle with criminal offences as, where the investigation concerns a criminal offence, the ground set out under point 3.3.2 would be applicable.

3.3.6 Monitoring, inspection or regulatory function connected to the exercise of official authority in the cases referred to in points (a) to (e) and (g) of Article 23 GDPR

The ground for restriction mentioned in Article 23(2)(h) GDPR refers to a potential limitation when there is an inspection or a monitoring exercise or a regulatory function connected, even if only

[9] See also paragraph 46 below.
[10] Recital 19 GDPR.
[11] Opinion 1/15 of the CJEU (Grand Chamber) on the Draft PNR Agreement between Canada and the European Union, 26 July 2017, ECLI:EU:C:2017:592.
[12] Recital 73 GDPR.

[13] Recital 73 GDPR.
[14] I.e. the data subject may ask the competent supervisory authority to proceed with the necessary checks and verifications of the information concerning the data subject. Such indirect access may be established for instance to protect security of the State, defence or public security. The Supervisory authority may then access and verify the information and where relevant can request rectification or deletion of the personal data being processed.

occasionally, to the exercise of official authority in the cases referred to in points 3.3.1 to 3.3.3 and 3.3.5.

3.3.7 Protection of the data subject or the rights and freedoms of others

33. Article 23(1)(i) GDPR refers to a ground for restriction that aims to protect the data subject or the rights and freedoms of other persons.

34. One can illustrate a restriction to protect the rights and freedoms of others with an example of an administrative inquiry and/or disciplinary proceedings or investigation on allegations of harassment in the workplace. In this case, a legislative measure may provide that the person subject to an inquiry or disciplinary proceedings may experience a limitation to his or her right of access, where the identity of an alleged victim or witness whistle-blower cannot be disclosed in order to protect him or her from retaliation. The victim or witness may also see his or her right of access restricted to respect the rights to privacy and data protection of the person subject to an inquiry or disciplinary proceedings.

3.3.8 Enforcement of civil law claims

35. Article 23(1)(j) GDPR also includes the enforcement of civil law claims as a ground for restrictions. While Article 23(1)(j) GDPR allows limitations to protect the individual interests of a (potential) litigant, Article 23(1)(f) GDPR allows limitations to protect the court proceedings themselves as well as the applicable procedural rules.

3.4 Data subjects' rights and controller's obligations which may be restricted

36. In accordance with Article 23 GDPR, only Articles 12 to 22, Article 34 GDPR and Article 5 as far as its provisions correspond to the rights and obligations provided for in Article 12 to 22 can be restricted.

37. The restrictions to obligations concern restrictions to the principles relating to the processing of personal data as far as the provisions of Article 5 correspond to the obligations provided in Article 12 to 22 GDPR and to the communication of a personal data breach to the data subjects (Article 34 GDPR). Article 5 GDPR, which establishes the principles relating to the processing of personal data, is one of the most important articles in the GDPR. Restrictions to the data protection principles need to be duly justified by an exceptional situation, respecting the essence of the fundamental rights and freedoms at issue and following a necessity and proportionality test[15] (see section 3.5 below). It should be noted that Article 5 GDPR can be only restricted in so far as its provisions correspond to the rights and obligations provided in Articles 12 to 22 GDPR.

38. The restrictions to rights concern the right to transparent information (Article 12 GDPR), right to information (Articles 13 and 14 GDPR), right of access (Article 15 GDPR), right to rectification (Article 16 GDPR), right to erasure (Article 17 GDPR), right to restriction of processing (Article 18 GDPR), notification obligation regarding rectification or erasure of personal data or restriction of processing (Article 19 GDPR), right to data portability (Article 20 GDPR), right to object (Article 21 GDPR), right not to be subject to an automated individual decision making (Article 22 GDPR).

39. This means that any other data subjects' rights - such as the right to lodge a complaint to the supervisory authority (Article 77 GDPR) - or other controllers' obligations cannot be restricted.

3.5 Necessity and proportionality test

[15] See European Data Protection Supervisor (EDPS) Guidelines - 'Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit', the EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data and the EDPS quick-guide to necessity and proportionality.

40. Restrictions are only lawful when they are a necessary and proportionate measure in a democratic society, as stated in Article 23(1) GDPR. This means that restrictions need to pass a necessity and proportionality test in order to be compliant with the GDPR[16]. The necessity and proportionality test should be carried out before the legislator decides to provide for a restriction.

41. The objective to be safeguarded provides the background against which the necessity of the measure may be assessed. It is therefore important to identify the objective in sufficient detail so as to allow the assessment on whether the measure is necessary. For example, if in administrative proceedings it is necessary to restrict part of the investigation, but some information can already be disclosed to the data subjects concerned, then that information should be provided to the person. The case law of the CJEU applies a strict necessity test for any limitations on the exercise of the rights to personal data protection and respect for private life with regard to the processing of personal data: 'derogations and limitations in relation to the protection of personal data (...) must apply only insofar as is strictly necessary'[17]. The ECtHR applies a test of strict necessity depending on the context and all circumstances at hand, such as with regard to secret surveillance measures[18].

42. If this test is satisfied, the proportionality of the envisaged measure will be assessed. Should the draft measure not pass the necessity test, there is no need to examine its proportionality. A measure which is not proved to be necessary should not be proposed unless and until it has been modified to meet the requirement of necessity.

43. The necessity and proportionality test typically implies assessing the risks to the rights and freedoms of the data subjects. The risks to the rights and freedoms of data subjects are detailed in point 4.7 of these guidelines.

44. According to the proportionality principle, the content of the legislative measure cannot exceed what is strictly necessary to safeguard the objectives listed in Article 23(1)(a) to (j) GDPR. The restriction must therefore be appropriate for attaining the legitimate objectives pursued by the legislation at issue and not exceed the limits of what is appropriate and necessary in order to achieve those objectives. According to the CJEU case law, Article 23 GDPR cannot be interpreted as being capable of conferring on Member States the power to undermine respect for private life, disregarding Article 7 of the Charter, or any of the other guarantees enshrined therein. In particular, the power conferred on Member States by Article 23(1) GDPR may be exercised only in accordance with the requirement of proportionality, according to which derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary[19].

45. A proposed restriction measure should be supported by evidence describing the problem to be addressed by that measure, how it will be addressed by it, and why existing or less intrusive measures cannot sufficiently address it. There is also a requirement to demonstrate how any proposed

[16] Within the mission of the supervisory authorities and in order to ensure legal certainty it is advisable that the proportionality and necessity test is documented. Supervisory authorities may request additional documentation.
[17] See CJEU, Judgment of 16 December 2008, case C-73/07, Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy, ECLI:EU:C:2008:727, paragraph 56.
[18] See ECtHR, Szabo and Vissy v. Hungary, 12 January 2016, paragraph 73.
[19] CJEU, judgment of 6 October 2020, La Quadrature du net and others joined cases C-511/18, C-512/18 and C-520/18, ECLI:EU:C:2020:791, paragraph 210. For example, in relation to data retention by online public communication services and hosting services providers, the CJEU concluded, paragraph 212, that 'Article 23(1) (GDPR), read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation which requires that providers of access to online public communication services and hosting service providers retain, generally and indiscriminately, inter alia, personal data relating to those services'.

interference or restriction genuinely meet objectives of general interest of the State and EU or the need to protect the rights and freedoms of others. The restriction of data protection rights will need to focus on specific risks.

46. For example, if restrictions contribute to safeguarding public health in a state of emergency, the EDPB considers that the restrictions must be strictly limited in scope (e.g. as to the purpose, data subject rights concerned or the categories of controllers concerned) and in time. In particular, it must be limited to the emergency state period. Data subject rights can be restricted but not denied.

4 REQUIREMENTS OF ARTICLE 23(2) GDPR

47. According to the CJEU case law, any legislative measure adopted on the basis of Article 23(1) GDPR must, in particular, comply with the specific requirements set out in Article 23(2) of the GDPR[20]. Article 23(2) GDPR states that the legislative measures imposing restrictions to the rights of data subjects and the controllers' obligations shall contain, where relevant, specific provisions about several criteria outlined below. As a rule, all the requirements detailed below should be included in the legislative measure imposing restrictions under Article 23 GDPR.

48. Exceptions to this rule, based on the fact that one or more provisions in Article 23(2) GDPR are not relevant regarding the legislative measure foreseeing the restriction of data subjects' rights, need to be duly justified by the legislator. The EDPB's interpretation of the expression "where relevant" in Article 23(2) GDPR is linked to the circumstances.

49. Article 23(2)(a) GDPR mentions the purposes of the processing or categories of processing as one of the specific provisions that shall be mentioned in any legislative measures restricting the rights of data subjects or controllers' obligations. As per Recital 8 GDPR, the reason for the restriction should be comprehensible to persons to whom it applies. This also involves a clear understanding of how and when the restriction may apply.

50. For example, national legislation on prevention and investigation of breaches of ethics for regulated professions might state that if the disclosure of the fact that a person is under investigation for a serious breach may be prejudicial to the purpose of the investigation, the information may not be disclosed to the data subject for a limited time.

51. The possible purposes of the processing need to be linked to the grounds for the restrictions mentioned in point 3.3 of these guidelines.

52. It should be said that sometimes the exercise of data subjects' rights helps the controllers performing their function. For example, the right to rectification can contribute to the quality of the data.

4.1 Categories of personal data

53. Article 23(2)(b) GDPR states that the categories of personal data subject to restrictions are to be indicated in the legislative measure foreseeing those restrictions[21].

[20] CJEU, judgment of 6 October 2020, La Quadrature du Net and others joined cases C-511/18, C-512/18 and C-520/18, ECLI:EU:C:2020:791, paragraph 209.
[21] Where possible, the controller can go further and list the specific data items to which the restriction of rights may apply, such as the preliminary results of an investigation, a decision opening an inquiry, etc.

54. In the same vein, restrictions concerning special categories of personal data may have a bigger impact on the data subjects and, therefore, the legislative measure setting such a restriction should mention the concerned special categories of data therein.

4.2 Scope of the restrictions

55. Article 23(2)(c) GDPR prescribes that the scope of the restrictions shall also be specified, i.e. which rights are concerned and how far they are going to be limited, for instance, that a restriction only concerns the right to restriction of processing (Article 18 GDPR), or that it may concern access, rectification and erasure.

4.3 Safeguards to prevent abuse or unlawful access or transfer

56. Article 23(2)(d) GDPR states that the legislative measure shall include safeguards to prevent abuse or unlawful access or transfer. This refers in particular to organisational and/or technical measures[22] which are necessary in order to avoid breaches or unlawful transfers such as the storage in a safe way of physical documents. For example, in some Member States the exercise of rights in respect of processing carried out in specific sectors can be exercised through the mediation of the national data protection supervisory authority ('SA').

57. The legislative measure may also concern periodic measures to review a given decision on restrictions. The legislator may propose that each restriction implemented by the controller should be reviewed periodically to ensure that the justification for it is still valid.

4.4 Specification of the controller

58. Article 23(2)(e) GDPR requires that the legislative measure specifies who the controller is or who the categories of controllers are. This appointment of the controllers in the legislative measure not only favours legal certainty regarding the responsibility for the processing operations in relation to the restrictions, but also allows data subjects to know whom to address when exercising their rights, once the restriction is lifted.

4.5 Storage periods

59. Article 23(2)(f) GDPR establishes that the legislative measure must include a specific provision regarding the storage periods and applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing. For instance, the retention period could be calculated as the duration of the processing operation plus additional time for potential litigation.

4.6 Risks to data subjects' rights and freedoms

60. Article 23(2)(g) GDPR requires that the legislative measure include the risks to data subject's rights and freedoms entailed by the restrictions. This is a very important step, which helps in the necessity and proportionality test of the restrictions.

61. The goal of this assessment of the risks to data subjects' rights and freedoms is twofold. On the one hand, it provides an overview of the potential impact of restrictions on data subjects. On the other hand, it provides elements for the necessity and proportionality test of the restrictions. In this regard and if applicable, a data protection impact assessment ('DPIA') should be considered[23].

[22] See EDPB Guidelines 4/2019 on Article 25 data protection by design and by default.
[23] See also Article 29 Working Party Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, wp248rev.01, endorsed by the EDPB on 25 may 2018.

62. The legislator should assess the risks to data subject's rights and freedoms from the perspective of the data subjects. It is not always mandatory to perform a DPIA, but concrete risks to data subjects - such as erroneous profiling leading to discrimination, reduced human dignity[24], freedom of speech, the right to privacy and data protection[25], a bigger impact on vulnerable groups (such as children or persons with disability), to mention a few - may be stated in the legislative measure, if applicable.

63. When such assessment is provided, the EDPB considers necessary to include it in the recitals or explanatory memorandum of the legislation[26] or in the impact assessment[27].

4.7 Right to be informed about the restriction, unless prejudicial to the purpose of the restriction

64. Article 23(2)(h) GDPR states that, unless it may be prejudicial to the purpose of the restriction, data subjects shall be informed of the restriction. This means that data subjects should be informed about the restriction to their right to information as a rule. To that purpose, a general data protection notice may be sufficient.

65. For example, where a data subject specifically asks to exercise a particular right at a very delicate moment of a given administrative investigation, the data subject should, if possible, be informed of the reasons for the restriction. However, if informing the data subject of the reasons for the restriction would result in cancelling the effect of the restriction (i.e. would hamper the preliminary effects of the investigation), that information may not be disclosed. Restrictions may be adopted to protect investigations. In this case, restrictions must remain necessary and proportionate and to do so an assessment should be performed by the controller to check whether informing the data subject of the restriction is prejudicial to the purpose of the restriction.

66. In other words, in extraordinary circumstances, for instance in the very preliminary stages of an investigation, if the data subject requests information if he or she is being investigated, the controller could decide not to grant that information at that moment - if this restriction is lawful and strictly necessary in the specific case to what would be prejudicial to the purpose of the restriction.

67. At a later stage, such as after the preliminary phase of the investigation or inquiry is completed, data subjects should receive a (specific) data protection notice. It is still possible at this stage that certain rights continue to be restricted, such as the right of access to the information about the opening of an investigation, or to the allegations of potential victims of harassment[28]. This fact should be indicated in the data protection notice along with an indication of a period in which the rights will be fully restored, if possible.

[24] Human dignity is a right protected by Article 1 of the Charter.
[25] Articles 7 and 8 of the Charter.
[26] The purpose of the explanatory memorandum is to explain the reasons for, and the context of a legislative measure drawing on the different stages of the preparatory process.
[27] See Article 35(10) GDPR.
[28] For further information, see CJEU, judgment of 17 July 2014, YS v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M and S, cases C-141/12 and C-372/12, ECLI:EU:C:2014:2081, paragraphs 45 and 46 and judgment of 20 December 2017, Novak, case C-434/16, ECLI:EU:C:2017:994, paragraph 56.

5 CONSULTATION WITH THE SAs (ARTICLES 36(4) AND 57(1)(C) GDPR)

68. In accordance with Article 36(4) GDPR, where restrictions are adopted at the level of the Member States, SAs shall be consulted before the adoption of the legislative measure to be adopted by a national parliament, or of a regulatory measure based on such a legislative measure envisaging the restriction of data subjects' rights under Article 23 GDPR.

69. Also, it is within the tasks of the SAs to provide advice on legislative measures relating to the protection of individuals' rights and freedoms regarding their personal data processing, in accordance with Article 57(1)(c) GDPR.

70. If SAs are not duly consulted, they can issue under Article 58(3)(b) GDPR on their own initiative opinions to the national parliament, the Member State government or, in accordance with Member State law, to other institutions or bodies as well as to the public on any issue related to the protection of personal data.

71. In addition, data protection legislation at national level may set out specific procedures regarding the adoption of legislative measures that aim at restricting the rights afforded by Artides 12 to 22 and Article 34 GDPR, in line with Article 23 GDPR. This could be the case only if in line with the GDPR.

6 NON - OBSERVATION OF ARTICLE 23 GDPR REQUIREMENTS BY A MEMBER STATE

72. The European Commission, as Guardian of the Treaties, has the duty to monitor the application of EU primary and secondary law and to ensure its uniform application throughout the EU, including by taking actions where national measures would fail to comply with EU law.

73. Furthermore, according to the principle of supremacy of EU law, the 'duty to disapply national legislation that is contrary to EU law is owed not only by national courts, but also by all organs of the State — including administrative authorities — called upon, within the exercise of their respective powers, to apply EU law'[29].

7 SPECIFIC ELEMENTS FOR CONTROLLERS AND PROCESSORS

7.1 Accountability Principle

74. In light of the accountability principle (Article 5(2) GDPR) and although it is not part of the records required under Article 30 GDPR, it is good practice that the controller documents the application of restrictions on concrete cases by keeping a record of their application. This record should include the applicable reasons for the restrictions, which ground(s) among those listed in Article 23(1) GDPR apply(ies) (where the legislative measure allows for restrictions on different grounds), its timing and the outcome of the necessity and proportionality test. The records should be made available on request to the data protection supervisory authority.

75. In case the controller has a data protection officer (DPO), the DPO should be informed - at least in a general manner - without undue delay whenever data subject rights are restricted in accordance with

[29] CJEU, judgment 4 December 2018, Case C-378/17, ECLI:EU:C:2018:979, paragraph 38.

the legislative measure. The DPO should be given access to the associated records and any documents concerning the factual or legal context in which the restriction takes place. The involvement of the DPO in the application of restrictions should also be documented.

7.2 Exercise of data subject's rights after the lifting of the restriction

76. The controller should lift the restrictions as soon as the circumstances that justify them no longer apply. If the data subjects have not yet been informed of the restrictions before that moment, they should be at the latest when the restriction is lifted.

77. During the application of a restriction, data subjects may be allowed to exercise all their rights, that are not restricted. In order to assess when the restriction can be partially or integrally lifted, a necessity and proportionality test may be performed several times during the application of a restriction.

78. When the restriction is lifted - which should be documented in the record mentioned in section 5 - data subjects can exercise all their rights.

79. If the controller does not allow data subjects to exercise their rights after the restriction has been lifted, the data subject can submit a complaint to the SA against the controller, in accordance with Article 57(1)(f) GDPR.

7.3 Non-observation of a legislative measure imposing such restrictions by a controller

80. Where the legislative measures imposing restrictions under Article 23 GDPR comply with the GDPR but are infringed by a controller, SAs can make use of their advisory, investigative and corrective powers against it, as in any other case of non-observation of GDPR rules.

81. In accordance with the powers foreseen in Article 58(1) GDPR, the SAs have the following investigative powers:

- order the controller and the processor, and, where applicable, the controller's or processor's representative to provide any information it requires for the performance of its tasks;
- carry out investigations in the form of data protection audits;
- notify the controller or the processor of an alleged infringement of the GDPR;
- obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks;
- obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law.

82. If corrective measures need to be applied, the SAs can in accordance with Article 58(2) GDPR:

- **issue warnings** to a controller or processor that intended processing operations are likely to infringe provisions of the GDPR;
- **issue reprimands** to a controller or a processor where processing operations have infringed provisions of the GDPR;
- **order** the controller or the processor **to comply** with the data subject's requests to exercise his or her rights pursuant to the GDPR;
- **order** the controller or processor **to bring processing operations into compliance** with the provisions of the GDPR, where appropriate, in a specified manner and within a specified period;
- **order** the controller **to communicate a personal data breach to the data subject**;
- **impose** a temporary or definitive limitation including **a ban** on processing;
- **order** the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 GDPR and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19 GDPR;

- **impose an administrative fine** pursuant to Article 83, in addition to, or instead of measures referred to in Article 58(2) GDPR, depending on the circumstances of each individual case;
- **order** the suspension of data flows to a recipient in a third country or to an international organisation.

83. Regarding the SAs advisory powers foreseen in Article 58(3) GDPR, they can:

- advice the controllers in accordance with the prior consultation procedure referred to in Article 36(1) and (5) GDPR;
- authorise processing referred to in Article 36(5) GDPR, if the law of the Member State requires such prior authorisation.

8 CONCLUSIONS

84. Article 23 GDPR allows under specific conditions, a national or Union legislator to restrict, by way of a legislative measure, the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 GDPR in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard, inter alia, important objectives of general public interest of the Union or of a Member State.

85. Restrictions of data subjects' rights need to observe the requirements stated in Article 23 GDPR. The Member States or the Union issuing the legislative measures setting those restrictions and the controllers applying them should be aware of the exceptional nature of these restrictions.

86. The proportionality test should be carried out before introducing in Union or Member State law restrictions on the rights of data subjects.

87. SAs should be consulted before the adoption of the legislative measures setting the restrictions and have the powers to enforce its compliance with the GDPR.

88. Once restrictions are lifted, data subjects must be allowed to exercise their rights by the controller.

9 ANNEX: CHECK-LISTS - ARTICLE 23 GDPR IN A NUTSHELL

9.1 Requirements under Article 23(1) GDPR

i. *Respect of the essence of the fundamental rights and freedoms*
ii. *Proportionality and necessity test*
iii. *Legislative measures laying down restrictions and the need to be foreseeable (Recital 41 and CJEU case law)*
iv. *Data subjects' rights and controller's obligations which may be restricted*
   a) the right to transparent information (Article 12 GDPR),
   b) right to information (Articles 13 and 14 GDPR),
   c) right of access (Article 15 GDPR),
   d) right to rectification (Article 16 GDPR),
   e) right to erasure (Article 17 GDPR),
   f) right to restriction of processing (Article 18 GDPR),
   g) notification obligation regarding rectification or erasure of personal data or restriction of processing (Article 19 GDPR),
   h) right to data portability (Article 20 GDPR),
   i) right to object (Article 21 GDPR),
   j) right not to be subject to an automated individual decision making (Article 22 GDPR)
   k) obligations provided in Article 12 to 22 GDPR (Article 5 GDPR) and
   l) the communication of a personal data breach to the data subjects (Article 34 GDPR)
v. *Grounds for the restrictions*
   a) national security;
   b) defence;
   c) public security;
   d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;
   e) other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation a matters, public health and social security;
   f) the protection of judicial independence and judicial proceedings;
   g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;
   h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g);
   i) the protection of the data subject or the rights and freedoms of others;
   j) the enforcement of civil law claims.

9.2 Requirements under Article 23(2) GDPR

i. *The purposes of the processing or categories of processing;*
ii. *The categories of personal data;*
iii. *The scope of the restrictions introduced;*
iv. *The safeguards to prevent abuse or unlawful access or transfer;*
v. *The specification of the controller or categories of controllers;*

vi. *The storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;*
vii. *The risks to the rights and freedoms of data subjects; and*
viii. *The right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.*



Wytyczne 09/2020 dotyczące mającego znaczenie dla sprawy i uzasadnionego sprzeciwu na podstawie rozporządzenia 2016/679

Wersja 2.0

Przyjęto 9 marca 2021 r.

Tabela zawierająca informacje o wersji

Wersja 1.0	8 października 2020 r.	Przyjęcie wytycznych do konsultacji publicznych
Wersja 2.0	9 marca 2021 r.	Przyjęcie wytycznych po konsultacjach publicznych

Spis treści

1 INFORMACJE OGÓLNE 4
2 WARUNKI „MAJĄCEGO ZNACZENIE DLA SPRAWY I UZASADNIONEGO" SPRZECIWU 6
2.1 „Mający znaczenie dla sprawy" 6
2.2 „Uzasadniony" 7
3 ISTOTA SPRZECIWU 8
3.1 Występowanie naruszenia RODO lub zgodność planowanego działania z RODO 8
3.1.1 Występowanie naruszenia RODO 9
3.1.2 Zgodność z RODO działania przewidzianego w projekcie decyzji w odniesieniu do administratora lub podmiotu przetwarzającego 11
3.2 Waga wynikającego z projektu decyzji ryzyka naruszenia podstawowych praw lub wolności osób, których dane dotyczą, oraz gdy ma to zastosowanie – waga ryzyka zakłócenia swobodnego przepływu danych osobowych w Unii 11
3.2.1 Znaczenie „wagi ryzyka" 12
3.2.2 Ryzyko naruszenia podstawowych praw i wolności osób, których dane dotyczą 12
3.2.3 Ryzyko zakłócenia swobodnego przepływu danych osobowych w Unii 13

Europejska Rada Ochrony Danych

uwzględniając art. 70 ust. 1 lit. e) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (zwanego dalej „RODO"),

uwzględniając Porozumienie EOG, w szczególności załącznik XI i protokół 37 do tego Porozumienia, zmienione decyzją Wspólnego Komitetu EOG nr 154/2018 z dnia 6 lipca 2018 r.[1],

uwzględniając art. 12 i art. 22 swojego regulaminu wewnętrznego,

PRZYJMUJE NASTĘPUJĄCE WYTYCZNE:

1 INFORMACJE OGÓLNE

1. W ramach mechanizmu współpracy określonego w RODO organy nadzorcze „wymieniają się wszelkimi stosownymi informacjami" i współpracują „w celu osiągnięcia porozumienia"[2]. Ten obowiązek współpracy dotyczy wszystkich etapów procedury, począwszy od rozpoczęcia sprawy, i obejmuje cały proces podejmowania decyzji. Osiągnięcie porozumienia dotyczącego wyniku sprawy jest zatem ostatecznym celem całej procedury ustanowionej w art. 60 RODO. Jeżeli organy nadzorcze nie osiągną porozumienia, EROD jest uprawniona do przyjmowania wiążących decyzji na podstawie art. 65 RODO. Wymiana informacji i konsultacje między wiodącym organem nadzorczym a organami nadzorczymi, których sprawa dotyczy, często umożliwiają osiągnięcie porozumienia na wczesnych etapach sprawy.

2. Zgodnie z art. 60 ust. 3 i 4 RODO wiodący organ nadzorczy przekazuje projekt decyzji organom nadzorczym, których sprawa dotyczy; te ostatnie mogą w określonym terminie (cztery tygodnie) zgłosić mający znaczenie dla sprawy i uzasadniony sprzeciw[3]. Po otrzymaniu mającego znaczenie dla sprawy i uzasadnionego sprzeciwu wiodący organ nadzorczy ma do wyboru dwie możliwości. Jeżeli nie przychyla się do mającego znaczenie dla sprawy i uzasadnionego sprzeciwu lub sądzi, że sprzeciw nie ma znaczenia dla sprawy lub nie jest uzasadniony – przekazuje sprawę EROD w ramach mechanizmu spójności. Jeżeli zaś wiodący organ nadzorczy przychyla się do sprzeciwu i wydaje zmieniony projekt decyzji, organy nadzorcze, których sprawa dotyczy, mogą wyrazić mający znaczenie dla sprawy i uzasadniony sprzeciw dotyczący zmienionego projektu decyzji w terminie dwóch tygodni.

3. Jeżeli wiodący organ nadzorczy nie przychyli się do sprzeciwu lub odrzuci taki sprzeciw jako niemający znaczenia dla sprawy lub nieuzasadniony, a co za tym idzie, przekaże sprawę EROD zgodnie z art. 65 ust. 1 lit. a) RODO, na EROD spoczywa obowiązek przyjęcia wiążącej decyzji w kwestii, czy sprzeciw „ma znaczenie dla sprawy i jest uzasadniony". W przypadku przyjęcia decyzji pozytywnej EROD jest zobowiązana do przyjęcia wiążącej decyzji dotyczącej wszystkich spraw będących przedmiotem sprzeciwu.

[1] Odniesienia do „państw członkowskich" zawarte w niniejszym dokumencie należy rozumieć jako odniesienia do „państw członkowskich EOG".
[2] Rozporządzenie 2016/679, zwane dalej „RODO", art. 60 ust. 1.
[3] Organy nadzorcze, których sprawa dotyczy, mają możliwość wycofywania wcześniej zgłoszonych sprzeciwów.

4. Jednym z kluczowych elementów oznaczających brak porozumienia między wiodącym organem nadzorczym a organami nadzorczymi, których sprawa dotyczy, jest zatem pojęcie „mającego znaczenie dla sprawy i uzasadnionego sprzeciwu". Celem niniejszego dokumentu jest przedstawienie wytycznych dotyczących tego pojęcia i ustalenie jednolitego rozumienia znaczenia terminów „mający znaczenie dla sprawy i uzasadniony", w tym określenie kwestii, które należy uwzględnić przy dokonywaniu oceny, czy sprzeciw „jasno wskaz[uje] wagę wynikającego z projektu decyzji ryzyka" (art. 4 pkt 24 RODO).

5. W art. 4 pkt 24 RODO zdefiniowano „mający znaczenie dla sprawy i uzasadniony sprzeciw" jako sprzeciw wobec projektu decyzji dotyczącej tego, czy doszło do naruszenia tego rozporządzenia lub czy planowane działanie wobec administratora lub podmiotu przetwarzającego jest zgodne z tym rozporządzeniem, który to sprzeciw musi jasno wskazywać wagę wynikającego z projektu decyzji ryzyka naruszenia podstawowych praw lub wolności osób, których dane dotyczą, oraz gdy ma to zastosowanie – wagę ryzyka zakłócenia swobodnego przepływu danych osobowych w Unii.

6. Pojęcie to służy jako **próg** w sytuacjach, w których organy nadzorcze, których sprawa dotyczy, zamierzają zgłosić sprzeciw wobec (zmienionego) projektu decyzji, który ma zostać przyjęty przez wiodący organ nadzorczy na podstawie art. 60 RODO. Niewiedza na temat tego, „czym jest mający znaczenie dla sprawy i uzasadniony sprzeciw", może prowadzić do nieporozumień i niespójnego stosowania przepisów przez organy nadzorcze. Prawodawca Unii zasugerował zatem, aby EROD wydała wytyczne dotyczące tego pojęcia (koniec motywu 124 RODO).

7. Aby osiągnąć próg określony w art. 4 pkt 24 RODO, zgłoszenie dokonane przez organ nadzorczy, którego sprawa dotyczy, powinno co do zasady wyraźnie wymieniać każdy element definicji w odniesieniu do każdego konkretnego sprzeciwu. **Celem sprzeciwu jest zatem przede wszystkim wskazanie, w jaki sposób i dlaczego, w opinii organu nadzorczego, którego sprawa dotyczy, projekt decyzji nie uwzględnia w odpowiedni sposób sytuacji naruszenia RODO lub nie przewiduje odpowiednich działań wobec administratora lub podmiotu przetwarzającego w świetle wykazanego ryzyka naruszenia podstawowych praw lub wolności osób, których dane dotyczą, oraz, w stosownych przypadkach, ryzyka zakłócenia swobodnego przepływu danych osobowych w Unii, które to ryzyko wynikałoby z projektu decyzji, jeżeli projekt ten pozostałby niezmieniony**. W zgłaszanym sprzeciwie organ nadzorczy, którego sprawa dotyczy, powinien wskazać każdą część projektu decyzji, którą uznał za wadliwą, błędną lub wykazującą brak niezbędnych elementów, albo poprzez odniesienie do określonych artykułów/ustępów, albo poprzez inne jasne odniesienia, oraz wykazać, dlaczego kwestie te należy uznać za „mające znaczenie dla sprawy", jak szerzej wyjaśniono poniżej. Przedstawione w sprzeciwie wnioski o wprowadzenie zmian powinny mieć na celu naprawienie tych potencjalnych błędów.

8. Na **stopień szczegółowości sprzeciwu i szczegółowość zawartej w nim analizy może jednak mieć wpływ stopień szczegółowości projektu decyzji oraz stopień zaangażowania organu nadzorczego, którego sprawa dotyczy**, w proces prowadzący do sporządzenia projektu decyzji wydanego przez wiodący organ nadzorczy. Norma, jaką stanowi „mający znaczenie dla sprawy i uzasadniony sprzeciw", opiera się na założeniu, że wiodący organ nadzorczy przestrzega obowiązku w zakresie wymiany wszelkich stosownych informacji[4], umożliwiając organom nadzorczym, których sprawa dotyczy, dogłębne zrozumienie sprawy, a co za tym idzie – zgłoszenie solidnego i dobrze uzasadnionego sprzeciwu. W związku z tym należy mieć również na uwadze konieczność „podawania powodów zastosowania środka" (zob. motyw 129 RODO) w przypadku każdego prawnie wiążącego środka zastosowanego przez organy nadzorcze. Stopień zaangażowania organu nadzorczego, którego sprawa dotyczy, przez wiodący organ nadzorczy w proces prowadzący do sporządzenia projektu decyzji – jeżeli na podstawie takiego stopnia zaangażowania nie uzyskano wystarczającej znajomości wszystkich aspektów sprawy – można zatem uznać za czynnik umożliwiający ustalenie w sposób bardziej elastyczny stopnia szczegółowości mającego znaczenie dla sprawy i uzasadnionego sprzeciwu.

[4] Zgodnie z art. 60 ust. 1 RODO.

9. EROD chce przede wszystkim podkreślić, że wszystkie zaangażowane organy nadzorcze (wiodący organ nadzorczy i organy nadzorcze, których sprawa dotyczy) powinny skupiać się na eliminowaniu wszelkich niedociągnięć w procesie dążenia do porozumienia, tak aby w efekcie jego osiągnięcia powstał projekt decyzji. EROD przyznaje, że zgłaszanie sprzeciwu nie jest najbardziej preferowanym narzędziem służącym poprawie niedostatecznego stopnia współpracy na poprzednich etapach postępowania w ramach kompleksowej współpracy, uznaje jednak jednocześnie, że jest to opcja, z której mogą skorzystać organy nadzorcze, których sprawa dotyczy. Jest to również środek ostateczny pozwalający na wyeliminowanie (domniemanych) niedociągnięć dotyczących zaangażowania organów nadzorczych, których sprawa dotyczy, przez wiodący organ nadzorczy w proces, który powinien był doprowadzić do sporządzenia projektu decyzji opartego na porozumieniu, w tym niedociągnięć dotyczących rozumowania prawnego i zakresu dochodzeń przeprowadzonych w danej sprawie przez wiodący organ nadzorczy.

10. W RODO przewidziano wymóg, aby organ nadzorczy, którego sprawa dotyczy, uzasadnił swoje stanowisko dotyczące projektu decyzji wydanej przez wiodący organ nadzorczy poprzez zgłoszenie sprzeciwu, który „ma znaczenie dla sprawy" i jest „uzasadniony". Należy mieć na uwadze, że oba wymogi – „mający znaczenie dla sprawy" i „uzasadniony" – powinno się uznać za **łączne**, tzn. oba z nich muszą być spełnione[5]. W art. 60 ust. 4 przewidziano zatem wymóg, aby wiodący organ nadzorczy przekazał sprawę do EROD w ramach mechanizmu spójności, jeżeli sądzi, że sprzeciw nie spełnia co najmniej jednego z tych dwóch elementów[6].

11. EROD zdecydowanie zaleca organom nadzorczym, aby dokonywały zgłoszeń sprzeciwu i wymiany informacji za pomocą ustanowionego systemu służącego do przekazywania i wymiany informacji między organami nadzorczymi[7]. Informacje powinny być w wyraźny sposób odpowiednio oznaczone za pomocą specjalnych funkcji i narzędzi do tego przeznaczonych.

2 WARUNKI „MAJĄCEGO ZNACZENIE DLA SPRAWY I UZASADNIONEGO" SPRZECIWU

2.1 „Mający znaczenie dla sprawy"

12. Aby sprzeciw został uznany za „mający znaczenie dla sprawy", musi występować **bezpośrednie powiązanie między sprzeciwem a istotą danego projektu decyzji**[8]. Mówiąc bardziej konkretnie, sprzeciw musi **dotyczyć albo ewentualnego naruszenia RODO, albo tego, czy planowane działanie wobec administratora albo podmiotu przetwarzającego jest zgodne z RODO**.

13. Zgłoszony sprzeciw spełnia zatem kryterium „mającego znaczenie dla sprawy", jeżeli przychylenie się do niego spowodowałoby wyciągnięcie **odmiennego wniosku** w kwestii ewentualnego naruszenia

[5] Zob. brzmienie art. 60 ust. 4 RODO.

[6] Zgodnie z art. 60 ust. 4 RODO wiodący organ nadzorczy przekazuje sprawę w ramach mechanizmu spójności, o którym mowa w art. 63, również jeżeli nie przychyla się do mającego znaczenie dla sprawy i uzasadnionego sprzeciwu.

[7] Zob. Regulamin Europejskiej Rady Ochrony Danych.

[8] Oksfordzki słownik języka angielskiego (Oxford English Dictionary) podaje definicję określenia „mający znaczenie dla sprawy" (ang. „relevant") jako *mający znaczenie dla danej sprawy lub powiązany z daną sprawą; mający ścisły związek z omawianym tematem lub kwestią; odnoszący się do określonej rzeczy* („relevant", przymiotnik, *OED Online*, Oxford University Press, czerwiec 2020 r., www.oed.com/view/Entry/161893. Dostęp 24 lipca 2020 r.).

RODO lub w kwestii tego, czy planowane działanie wobec administratora albo podmiotu przetwarzającego, proponowane przez wiodący organ nadzorczy, jest zgodne z RODO. Między treścią sprzeciwu a ewentualnym odmiennym wnioskiem musi zawsze występować powiązanie, jak objaśniono szerzej poniżej. Chociaż istnieje możliwość zgłoszenia w sprzeciwie różnicy zdań dotyczącej obu elementów, istnienie takiej różnicy w odniesieniu do tylko jednego z tych elementów byłoby wystarczające do spełnienia warunków sprzeciwu mającego znaczenie dla sprawy.

14. Sprzeciw należy uznać za mający znaczenie dla sprawy wyłącznie w przypadku, gdy odnosi się on do konkretnej prawnej i merytorycznej treści projektu decyzji wydanej przez wiodący organ nadzorczy. Abstrakcyjnych lub ogólnych obaw lub uwag nie można uznać w tym kontekście za mające znaczenie dla sprawy. Podobnie niewielkich różnic zdań dotyczących brzmienia projektu decyzji lub rozumowania prawnego, które nie odnoszą się do ewentualnego wystąpienia naruszenia RODO ani do zgodności z RODO planowanego działania wobec administratora albo podmiotu przetwarzającego, nie powinno uznawać się za mające znaczenie dla sprawy.

15. Rozumowanie, na którym wiodący organ nadzorczy opiera wnioski zawarte w projekcie decyzji, może być przedmiotem sprzeciwu, lecz tylko w zakresie, w jakim rozumowanie to powiązane jest z wnioskiem co do tego, czy doszło do naruszenia, czy naruszenie RODO prawidłowo wykazano lub czy rozumowanie to jest powiązane ze zgodnością planowanego działania z RODO, oraz pod warunkiem, że osiągnięto w całości próg określony w art. 4 pkt 24, opisany w niniejszym dokumencie.

2.2 „Uzasadniony"

16. Aby sprzeciw był „uzasadniony"[9], musi zawierać wyjaśnienia i argumenty tłumaczące, **dlaczego proponuje się zmianę decyzji** (tj. błędy prawne/merytoryczne w projekcie decyzji sporządzonym przez wiodący organ nadzorczy). Musi również wykazywać, **w jaki sposób zmiana prowadziłaby do odmiennego wniosku** w kwestii występowania naruszenia RODO lub w kwestii tego, czy planowane działanie wobec administratora albo podmiotu przetwarzającego jest zgodne z RODO.

17. Organ nadzorczy, którego sprawa dotyczy, powinien przedstawić solidne i umotywowane uzasadnienie sprzeciwu, podając szczegółowo **argumenty prawne** (na podstawie prawa Unii lub właściwego prawa krajowego, z uwzględnieniem np. przepisów prawnych, orzecznictwa, wytycznych) lub, w stosownych przypadkach, **fakty**. Organ nadzorczy, którego sprawa dotyczy, powinien przedstawić fakty, które w jego ocenie prowadzą do wyciągnięcia odmiennego wniosku w odniesieniu do naruszenia RODO przez administratora/podmiot przetwarzający, lub aspekt projektu decyzji, który, jego zdaniem, jest wadliwy/błędny.

18. Sprzeciw jest ponadto „uzasadniony" w zakresie, w jakim jest w stanie **„jasno wskazać" wagę ryzyka wynikającego z projektu decyzji**, jak opisano w sekcji 3.2 poniżej. W tym celu sprzeciw musi przedstawiać argumenty lub uzasadnienia dotyczące skutków wydania decyzji bez wprowadzenia zmian proponowanych w sprzeciwie oraz tego, w jaki sposób skutki te stwarzałyby istotne ryzyko naruszenia podstawowych praw lub wolności osób, których dane dotyczą, oraz, w stosownych przypadkach, istotne ryzyko zakłócenia swobodnego przepływu danych osobowych w Unii.

19. Aby sprzeciw był należycie uzasadniony, musi zawierać **spójne, jasne, precyzyjne i szczegółowe wytłumaczenie przyczyn zgłoszenia sprzeciwu**. W sprzeciwie należy przedstawić w sposób jasny i precyzyjny **główne elementy**, na których organ nadzorczy, którego sprawa dotyczy, oparł swoją ocenę, oraz **powiązanie między przewidywanymi skutkami projektu decyzji** (jeżeli wydano by ją

[9] Oksfordzki słownik języka angielskiego (Oxford English Dictionary) podaje definicję słowa „uzasadniony" (ang. „reasoned") jako „charakteryzujący się rozumowaniem lub oparty na rozumowaniu; uważnie zbadany" („reasoned", przymiotnik ZOED Online, Oxford University Press, czerwiec 2020 r., www.oed.com/view/Entry/159078.Dostęp 24 lipca 2020 r.).

w obecnej formie) **a wagą przewidywanego ryzyka naruszenia podstawowych praw lub wolności osób, których dane dotyczą, oraz – w stosownych przypadkach – wagę ryzyka zakłócenia swobodnego przepływu danych osobowych w Unii**. Organ nadzorczy, którego sprawa dotyczy, powinien ponadto **jasno wskazać, które części projektu decyzji są przedmiotem różnicy zdań**. W przypadku gdy podstawą sprzeciwu jest opinia, że wiodący organ nadzorczy nie zbadał w pełni ważnego faktu dotyczącego sprawy lub dodatkowego naruszenia RODO, wystarczyłoby, aby organ nadzorczy, którego sprawa dotyczy, przedstawił odnośne argumenty w sposób jednoznaczny i umotywowany.

20. Aby skutecznie przedstawić swoją argumentację, organy nadzorcze, których sprawa dotyczy, muszą przekazać wszystkie informacje (fakty, dokumenty, argumenty prawne), na których się opierają. Ma to zasadnicze znaczenie dla wyznaczenia zakresu (potencjalnego) sporu. Oznacza to, że **co do zasady organ nadzorczy, którego sprawa dotyczy, powinien dążyć do przekazania mającego znaczenie dla sprawy i uzasadnionego sprzeciwu w postaci jednego zgłoszenia** popartego wszystkimi merytorycznymi i legalnymi argumentami, które opisano powyżej. **Organ nadzorczy, którego sprawa dotyczy, może jednak w terminie określonym w art. 60 ust. 4 RODO przekazywać dodatkowe informacje związane ze zgłoszonym sprzeciwem i potwierdzające go, z uwzględnieniem konieczności przestrzegania wymogów określających, że sprzeciw musi „mieć znaczenie dla sprawy i być uzasadniony"**.

> **Przykład 1**: Organ nadzorczy, którego sprawa dotyczy, zgłasza formalny sprzeciw, lecz kilka dni później przekazuje wiodącemu organowi nadzorczemu dodatkowe informacje dotyczące faktów związanych ze sprawą za pośrednictwem systemu służącego do przekazywania i wymiany informacji. Wiodący organ nadzorczy może uwzględnić te informacje wyłącznie w przypadku, gdy zostały one przekazane w terminie określonym w art. 60 ust. 4 RODO.

21. W ramach dobrej praktyki sprzeciw powinien w miarę możliwości zawierać **proponowane nowe brzmienie** do rozważenia przez wiodący organ nadzorczy, które to brzmienie, zdaniem organu nadzorczego, którego sprawa dotyczy, pozwala wyeliminować domniemane niedociągnięcia w projekcie decyzji. Działanie takie może służyć lepszemu wyjaśnieniu sprzeciwu w odpowiednim kontekście.

3 ISTOTA SPRZECIWU

22. Przedmiot sprzeciwu może dotyczyć ewentualnego naruszenia RODO lub tego, czy planowane działanie wobec administratora albo podmiotu przetwarzającego jest zgodne z RODO. Rodzaj treści będzie zależał od przedmiotowego projektu decyzji wiodącego organu nadzorczego oraz od okoliczności sprawy.

23. Sprzeciw organu nadzorczego, którego sprawa dotyczy, musi ponadto jasno wskazywać wagę wynikającego z projektu decyzji ryzyka naruszenia podstawowych praw lub wolności osób, których dane dotyczą, oraz gdy ma to zastosowanie – wagę ryzyka zakłócenia swobodnego przepływu danych osobowych w Unii. Występowanie naruszenia lub niezgodności planowanego działania z RODO należy oceniać w świetle wagi ryzyka naruszenia podstawowych praw lub wolności osób, których dane dotyczą, oraz, w stosownych przypadkach, ryzyka zakłócenia swobodnego przepływu danych osobowych w Unii, wynikających z projektu decyzji, o ile pozostanie on niezmieniony.

3.1 Występowanie naruszenia RODO lub zgodność planowanego działania z RODO

3.1.1 Występowanie naruszenia RODO

24. W pierwszym przypadku istotą sprzeciwu będzie różnica zdań między organem nadzorczym, którego sprawa dotyczy, a wiodącym organem nadzorczym w kwestii tego, czy w ramach przedstawionych faktów czynności i operacje przetwarzania dokonane przez administratora lub podmiot przetwarzający doprowadziły do naruszenia RODO, a jeżeli tak, to do jakich konkretnie naruszeń.

25. W tym kontekście termin „naruszenie" należy interpretować jako „naruszenie określonego przepisu RODO". Sprzeciw organu nadzorczego, którego sprawa dotyczy, wobec projektu decyzji musi być zatem uzasadniony i umotywowany przez odniesienie do dowodów i faktów, które wiodący organ nadzorczy i organy nadzorcze, których sprawa dotyczy, wymieniły między sobą („stosowne informacje", o których mowa w art. 60 RODO). Wymogi te należy stosować do każdego naruszenia i do każdego odnośnego przepisu.

> **Przykład 2:** W projekcie decyzji stwierdzono, że administrator naruszył art. 6, 7 i 14 RODO. Organ nadzorczy, którego sprawa dotyczy, nie zgadza się w kwestii występowania naruszenia art. 7 i 14 oraz uważa, że dodatkowo naruszono art. 13 RODO.
>
> **Przykład 3:** Organ nadzorczy, którego sprawa dotyczy, argumentuje, że wiodący organ nadzorczy nie uwzględnił faktu, iż wyłączenie czynności o domowym charakterze nie ma zastosowania do niektórych operacji przetwarzania dokonywanych przez administratora i obejmujących używanie telewizji przemysłowej, zatem nie występuje naruszenie RODO. Aby uzasadnić swój sprzeciw, organ nadzorczy, którego sprawa dotyczy, powołuje się na art. 2 ust. 2 lit. c) RODO, wytyczne EROD 3/2019 w sprawie przetwarzania danych osobowych przez urządzenia wideo oraz wyrok TSUE w sprawie C-212/13 Ryneš.

26. Sprzeciw w kwestii wystąpienia naruszenia RODO może również obejmować różnicę zdań dotyczącą wniosków, jakie należy wyciągnąć z ustaleń dochodzenia. Sprzeciw może na przykład stwierdzać, że z ustaleń wynika naruszenie przepisu RODO inne niż te naruszenia, które zostały już zbadane w projekcie decyzji wiodącego organu nadzorczego (lub dodatkowe w stosunku do nich). Wystąpienie takiej sytuacji jest jednak mniej prawdopodobnie, jeżeli w czasie poprzedzającym wydanie projektu decyzji należycie przestrzegano obowiązku współpracy między wiodącym organem nadzorczym i organami nadzorczymi, których sprawa dotyczy, i wymiany wszelkich stosownych informacji, zgodnie z art. 60 ust. 1 RODO.

27. W pewnych okolicznościach w sprzeciwie można wręcz wskazać luki w projekcie decyzji uzasadniające potrzebę prowadzenia przez wiodący organ nadzorczy dalszego dochodzenia. Jeżeli na przykład dochodzenie przeprowadzone przez wiodący organ nadzorczy z nieuzasadnionych przyczyn nie obejmuje niektórych kwestii poruszonych przez skarżącego lub wynikających z naruszenia zgłoszonego przez organ nadzorczy, którego sprawa dotyczy, możliwe jest zgłoszenie mającego znaczenie dla sprawy i uzasadnionego sprzeciwu poprzez powołanie się na nienależyte rozpatrzenie skargi i niezabezpieczenie praw osoby, której dane dotyczą, przez wiodący organ nadzorczy. W tym zakresie należy rozróżnić, z jednej strony, postępowania z własnej inicjatywy, a z drugiej strony dochodzenia wszczęte na podstawie skarg lub zgłoszeń potencjalnych naruszeń przekazanych przez organy nadzorcze, których sprawa dotyczy. W procedurach na podstawie skargi lub naruszenia zgłoszonych przez organ nadzorczy, którego sprawa dotyczy, zakres procedury (tj. te aspekty przetwarzania danych, które stanowią potencjalnie przedmiot naruszenia) powinna określać treść skargi lub zgłoszenia przekazanego przez organ nadzorczy, którego sprawa dotyczy: innymi słowy powinno się go definiować na podstawie aspektów, do których odnosi się skarga lub zgłoszenie. W postępowaniach z własnej inicjatywy wiodący organ nadzorczy lub organy nadzorcze, których sprawa dotyczy, powinny dążyć do konsensusu, jeżeli chodzi o zakres procedury (tj. aspekty przetwarzania danych będącego przedmiotem kontroli) przed formalnym wszczęciem procedury. To samo dotyczy przypadków,

w których organ nadzorczy rozpatrujący skargę lub zgłoszenie innego organu nadzorczego stwierdza, że postępowanie z własnej inicjatywy jest niezbędne również po to, aby rozwiązać problemy systemowe w zakresie przestrzegania RODO wykraczające poza konkretną skargę lub zgłoszenie.

28. Jak wspomniano powyżej, zgłoszenie sprzeciwu należy rozważać wyłącznie jako ostateczność w celu zaradzenia rzekomo niewystarczającemu zaangażowaniu organów nadzorczych, których sprawa dotyczy, na wcześniejszych etapach procesu. Z systemu opracowanego przez prawodawcę wynika, że konsensus w sprawie zakresu dochodzenia powinny osiągnąć na wcześniejszym etapie właściwe organy nadzorcze.

29. Niewystarczające informacje lub opis przedmiotowej sprawy, brak oceny lub uzasadnienia, lub niewystarczające ocena lub uzasadnienie (w wyniku czego przeprowadzona ocena i przedstawione dowody nie stanowią odpowiedniego poparcia dla wniosku wiodącego organu nadzorczego zawartego w projekcie decyzji, jak wymaga tego art. 58 RODO) mogą być także przedmiotem sprzeciwu związanego z istnieniem naruszenia. Warunkiem jest, aby został osiągnięty w pełni próg określony w art. 4 pkt 24 RODO i aby było możliwe istnienie powiązania między taką rzekomo niewystarczającą analizą a stwierdzeniem naruszenia / planowanym działaniem.

30. W mającym znaczenie dla sprawy i uzasadnionym sprzeciwie można podnieść kwestie dotyczące aspektów proceduralnych w zakresie, w jakim dotyczą one sytuacji, w których wiodący organ nadzorczy rzekomo naruszył wymogi proceduralne nałożone przez RODO, co miało wpływ na wniosek sformułowany w projekcie decyzji.

> **Przykład 4**: Organ nadzorczy państwa członkowskiego YY może pełnić rolę wiodącego organu nadzorczego w przypadku transgranicznego przetwarzania prowadzonego przez administratora CC, którego główna jednostka organizacyjna znajduje się w YY. Właściwy organ nadzorczy państwa członkowskiego XX informuje wiodący organ nadzorczy (YY) o skardze wniesionej do organu nadzorczego XX, która w poważnym stopniu wpływa na osoby, których dane dotyczą, wyłącznie w XX zgodnie z art. 56 ust. 2 i 3 RODO. Wiodący organ nadzorczy decyduje, że zajmie się daną sprawą.
>
> Organ nadzorczy XX podejmuje decyzję o przedłożeniu wiodącemu organowi nadzorczemu projektu decyzji zgodnie z art. 56 ust. 4 RODO. Wiodący organ nadzorczy przygotowuje projekt decyzji zgodnie z art. 60 ust. 3 RODO i przedkłada go organowi nadzorczemu, którego sprawa dotyczy. Organ nadzorczy XX jest zdania, że podczas przygotowywania swojego projektu decyzji wiodący organ nadzorczy nie spełnił swojego obowiązku dotyczącego uwzględnienia w jak największym stopniu projektu przedłożonego przez organ nadzorczy XX zgodnie z art. 56 ust. 4 RODO, ponieważ nie przedstawił uzasadnienia powodów, dla których projekt decyzji wiodącego organu nadzorczego odbiega od projektu decyzji przedłożonego przez organ nadzorczy XX.
>
> Następnie organ nadzorczy XX zgłasza mający znaczenie dla sprawy i uzasadniony sprzeciw, w ramach którego przedstawia argumenty na poparcie innego wniosku, który byłby zawarty w projekcie decyzji, gdyby wiodący organ nadzorczy przychylił się do jego projektu decyzji, pod względem stwierdzenia naruszenia lub określenia działań przewidzianych wobec administratora, a także w celu uniknięcia wykazanego ryzyka naruszenia podstawowych praw lub wolności osoby, której dane dotyczą, oraz – w stosownych przypadkach – ryzyka zakłócenia swobodnego przepływu danych osobowych w Unii.

31. Sprzeciw zgłoszony zgodnie z art. 60 ust. 4 i art. 65 ust. 1 lit. a) RODO pozostaje bez uszczerbku dla przepisów art. 65 ust. 1 lit. b) RODO. W związku z tym braku porozumienia co do kompetencji organu nadzorczego pełniącego rolę wiodącego organu nadzorczego do wydania decyzji w danej sprawie nie należy podnosić poprzez sprzeciw na podstawie art. 60 ust. 4 RODO. Wspomniany brak porozumienia nie wchodzi również w zakres art. 4 pkt 24 RODO. Inaczej niż w przypadku sprzeciwu na podstawie

art. 60 ust. 4 RODO EROD uważa, że procedura określona w art. 65 ust. 1 lit. b) RODO może mieć zastosowanie na każdym etapie.

3.1.2 Zgodność z RODO działania przewidzianego w projekcie decyzji w odniesieniu do administratora lub podmiotu przetwarzającego

32. W tym drugim scenariuszu istota mającego znaczenie dla sprawy i uzasadnionego sprzeciwu jest równoznaczna z brakiem porozumienia, jeżeli chodzi o konkretne działanie naprawcze zaproponowane przez wiodący organ nadzorczy lub inne działanie przewidziane w projekcie decyzji.

33. Mówiąc bardziej konkretnie, mający znaczenie dla sprawy i uzasadniony sprzeciw powinien obejmować wyjaśnienie powodu, dla którego działanie przewidziane w projekcie decyzji nie jest zgodne z RODO. W związku z tym organ nadzorczy, którego sprawa dotyczy, musi wyraźnie określić fakty i argumenty prawne leżące u podstaw innej oceny sytuacji poprzez wskazanie, jakie działanie powinien podjąć i uwzględnić w swojej ostatecznej decyzji wiodący organ nadzorczy.

> **Przykład 5**: Administrator ujawnił stronie trzeciej wrażliwe dane medyczne skarżącego, nie mając do tego podstawy prawnej. W projekcie decyzji wiodący organ nadzorczy zaproponował udzielenie upomnienia, natomiast organ nadzorczy, którego sprawa dotyczy, przedstawił fakty świadczące o tym, że administrator boryka się z ogólnymi problemami systemowymi w zakresie przestrzegania RODO (np. regularnie ujawnia stronom trzecim dane swoich klientów, nie mając do tego podstawy prawnej). W związku z tym proponuje, aby nałożyć nakaz zapewnienia zgodności operacji przetwarzania z przepisami, tymczasowy zakaz przetwarzania danych lub karę pieniężną.
>
> **Przykład 6**: W wyniku błędu jednego z pracowników administrator opublikował na swojej stronie internetowej imiona, nazwiska i numery telefonów wszystkich swoich 100 000 klientów. Te dane osobowe były publicznie dostępne przez dwa dni. Ponieważ administrator zareagował tak szybko, jak to było możliwe, błąd zgłoszono, a wszystkich klientów indywidualnie powiadomiono o sytuacji, która zaszła, wiodący organ nadzorczy zamierzał udzielić administratorowi tylko upomnienia. Jeden z organów nadzorczych, których sprawa dotyczy, uważa jednak, że ze względu na dużą skalę naruszenia ochrony danych i ewentualny jego wpływ na życie prywatne klientów/ryzyko dla życia prywatnego klientów konieczne byłoby nałożenie kary pieniężnej.

34. Zgodnie z ostatnim zdaniem art. 65 ust. 1 lit. a) RODO wiążąca decyzja EROD dotyczy wszystkich spraw, które są przedmiotem sprzeciwu, w szczególności w przypadku naruszenia. W motywie 150 zdanie piąte RODO określono, że aby wspierać spójne stosowanie administracyjnych kar pieniężnych, można także użyć mechanizmu spójności. W związku z tym istnieje możliwość, że sprzeciw podważy elementy, na których podstawie obliczono kwotę kary pieniężnej. Jeżeli w ocenie EROD w tym kontekście zostaną zidentyfikowane niedociągnięcia w rozumowaniu prowadzącym do nałożenia przedmiotowej kary pieniężnej, wiodący organ nadzorczy zostanie poinstruowany, by przeprowadzić ponowną ocenę kary pieniężnej i wyeliminować zidentyfikowane niedociągnięcia. Ocena EROD w tej kwestii powinna opierać się na wspólnych normach EROD wynikających z art. 83 ust. 1 i 2 RODO oraz wytycznych w sprawie obliczania administracyjnych kar pieniężnych.

> **Przykład 7**: Organ nadzorczy, którego sprawa dotyczy, uważa, że – jeżeli uwzględni się okoliczności sprawy – kara pieniężna w wysokości przewidzianej przez wiodący organ nadzorczy w projekcie decyzji nie jest ani skuteczna, ani proporcjonalna, ani odstraszająca, jak wymaga tego art. 83 ust. 1 RODO.

3.2 Waga wynikającego z projektu decyzji ryzyka naruszenia podstawowych praw lub wolności osób, których dane dotyczą, oraz gdy ma to zastosowanie – waga ryzyka zakłócenia swobodnego przepływu danych osobowych w Unii

3.2.1 Znaczenie „wagi ryzyka"

35. Istotne jest, aby mieć na uwadze, że celem pracy wykonywanej przez organy nadzorcze jest ochrona podstawowych praw i wolności osób, których dane dotyczą, oraz ułatwianie swobodnego przepływu danych osobowych w Unii (art. 4 pkt 24, art. 51 i motyw 123 RODO).

36. **Obowiązek wykazania wagi wynikającego z projektu decyzji (np. ze środków przewidzianych w decyzji lub z braku działań naprawczych itp.) ryzyka naruszenia praw lub wolności osób, których dane dotyczą, oraz gdy ma to zastosowanie – wagi ryzyka zakłócenia swobodnego przepływu danych osobowych w Unii spoczywa na organie nadzorczym, którego sprawa dotyczy**. Możliwość wykazania tego przez organy nadzorcze, których sprawa dotyczy, zależy także od stopnia szczegółowości samego projektu decyzji oraz wcześniejszego przekazania informacji przez wiodący organ nadzorczy, jak podkreślono powyżej w pkt 8.

37. O „ryzyku" mowa jest w wielu sekcjach RODO, a we wcześniejszych wytycznych EROD[10] zdefiniowano je jako „scenariusz opisujący zdarzenie i jego konsekwencje oszacowane pod względem powagi i prawdopodobieństwa ryzyka". W art. 4 pkt 24 RODO odniesiono się do potrzeby wykazania „wagi" ryzyka związanego z projektem decyzji, tj. wykazania wpływu, jaki projekt decyzji miałby na chronione wartości. Organ nadzorczy, którego sprawa dotyczy, będzie musiał wykazać wagę ryzyka poprzez przedstawienie wystarczających argumentów, wyraźnie wskazujących, że takie ryzyko jest znaczące i prawdopodobne w odniesieniu do podstawowych praw i wolności osób, których dane dotyczą, oraz – w stosownych przypadkach – do swobodnego przepływu danych w Unii. Wykazana waga ryzyka nie może wynikać w dorozumiany sposób z argumentów prawnych lub faktów przedstawionych przez organ nadzorczy, którego sprawa dotyczy, ale musi być wyraźnie zidentyfikowana i omówiona w sprzeciwie.

38. Należy podkreślić, że choć w mającym znaczenie dla sprawy i uzasadnionym sprzeciwie należy zawsze wyraźnie wykazać wagę wynikającego z projektu decyzji ryzyka naruszenia podstawowych praw lub wolności osób, których dane dotyczą, (zob. sekcja 3.2.2 poniżej), wykazanie wagi ryzyka zakłócenia swobodnego przepływu danych osobowych w Unii Europejskiej jest wymagane tylko, „gdy ma to zastosowanie" (zob. sekcja 3.2.3 poniżej).

3.2.2 Ryzyko naruszenia podstawowych praw i wolności osób, których dane dotyczą

39. Przedmiotowa kwestia dotyczy wpływu, jaki projekt decyzji jako całość mógłby wywrzeć na podstawowe prawa i wolności osób, których dane dotyczą. Może to dotyczyć ustaleń dokonanych przez wiodący organ nadzorczy w odniesieniu do tego, czy administrator lub podmiot przetwarzający naruszyli przepisy RODO, lub wprowadzenia działań naprawczych.

40. Podejście, jakie należy zastosować podczas oceny ryzyka wynikającego z projektu decyzji, nie jest tym samym podejściem, jakie stosuje administrator podczas przeprowadzania oceny skutków dla ochrony danych w celu ustalenia ryzyka związanego z planowaną operacją przetwarzania. Przedmiot oceny jest w istocie zupełnie inny – przedmiotem oceny są mianowicie skutki wniosków wyciągniętych przez wiodący organ nadzorczy określone w jego projekcie decyzji dotyczące tego, czy doszło do naruszenia. Wnioski wiodącego organu nadzorczego mogą obejmować wdrożenie określonych środków („planowane działanie"). Jak już wspomniano, organ nadzorczy, którego sprawa dotyczy, musi wykazać takie ryzyko poprzez uwzględnienie projektu decyzji jako całości.

41. W motywie 129 RODO wyjaśniono, że „[s]woje uprawnienia organy nadzorcze powinny wykonywać zgodnie z odpowiednimi zabezpieczeniami proceduralnymi przewidzianymi w prawie Unii i prawie

[10] Zob. np. WP 248 rev.01, wytyczne dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko" do celów rozporządzenia 2016/67.

państwa członkowskiego, bezstronnie, sprawiedliwie i w rozsądnym terminie" oraz że „każdy środek powinien być odpowiedni, niezbędny i proporcjonalny, aby zapewnić przestrzeganie niniejszego rozporządzenia – z uwzględnieniem okoliczności danej sprawy, z poszanowaniem prawa do wysłuchania danej osoby przed zastosowaniem indywidualnego środka, który miałby niekorzystnie na nią wpłynąć, i bez nadmiernych kosztów i niedogodności dla danej osoby".

42. W związku z tym ocena wynikającego z projektu decyzji ryzyka naruszenia podstawowych praw i wolności osób, których dane dotyczą, może opierać się między innymi na prawidłowości, konieczności i proporcjonalności przewidzianych (lub nieprzewidzianych) w projekcie środków jako opierających się na ustaleniach związanych z istnieniem naruszenia oraz ewentualnych działań naprawczych określonych przez administratora lub podmiot przetwarzający.

43. Ponadto takie ryzyko może odnosić się do wpływu projektu decyzji na podstawowe prawa i wolności osób, których dane osobowe są przetwarzane przez administratora lub podmiot przetwarzający, ale także do wpływu na prawa i wolności osób, których dane osobowe mogą być przetwarzane w przyszłości, oraz do ewentualnych ograniczeń naruszeń przepisów RODO w przyszłości, tam gdzie przemawia za tym stan faktyczny.

Przykład 8: W projekcie decyzji wiodącego organu nadzorczego stwierdzono, że administrator nie naruszył zasady minimalizacji danych przewidzianej w art. 5 ust. 1 lit. c) RODO. Organ nadzorczy, którego sprawa dotyczy, podnosi w swoim sprzeciwie fakty i argumenty prawne, wykazując, że skutkiem przetwarzania dokonywanego przez administratora faktycznie było naruszenie art. 5 ust. 1 lit. c) RODO, oraz argumentując, że należy udzielić administratorowi upomnienia. W celu wykazania wagi ryzyka naruszenia podstawowych praw i wolności osób, których dane dotyczą, organ nadzorczy, którego sprawa dotyczy, argumentuje, że brak upomnienia za naruszenie podstawowej zasady stworzyłby niebezpieczny precedens, ponieważ nie sygnalizowałby konieczności naprawienia działań organizacji związanych z przetwarzaniem danych i zagrażałby osobom, których dane osobowe są i będą przetwarzane przez administratora.

3.2.3 Ryzyko zakłócenia swobodnego przepływu danych osobowych w Unii

44. Jeżeli sprzeciw odnosi się również do tego konkretnego ryzyka, organ nadzorczy, którego sprawa dotyczy, będzie musiał wyjaśnić, dlaczego uznaje się go za „mający zastosowanie". Ponadto sprzeciw, w którym zostanie wykazane ryzyko zakłócenia swobodnego przepływu danych osobowych w Unii, ale nie ryzyko naruszenia podstawowych praw i wolności osób, których dane dotyczą, nie zostanie uznany za sprzeciw, w którym osiągnięto próg określony w art. 4 pkt 24 RODO.

45. W RODO wyraźnie mowa jest o tym, że należy unikać ograniczania lub zakazu swobodnego przepływu danych osobowych z powodów odnoszących się do ochrony osób fizycznych w związku z przetwarzaniem danych osobowych[11]. Celem RODO jest wprowadzenie w całej UE zharmonizowanych przepisów o ochronie danych oraz umożliwienie swobodnego przepływu danych osobowych w Unii przy jednoczesnym zapewnieniu wysokiego stopnia ochrony podstawowych praw i wolności osób fizycznych, w szczególności ich prawa do ochrony swoich danych osobowych.

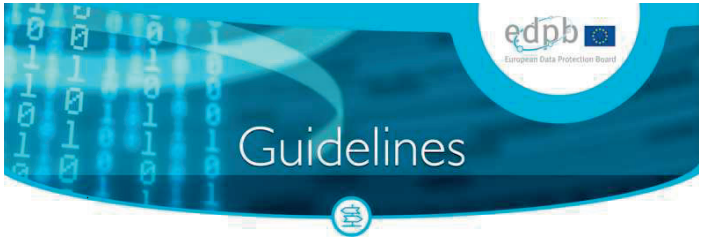
46. Ryzyko zakłócenia swobodnego przepływu danych osobowych w Unii mogą spowodować jakiekolwiek środki, w tym decyzje krajowych organów nadzorczych, w których wprowadza się nieuzasadnione ograniczenia dotyczące przechowywania danych (np. przepisy, w których zobowiązuje się administratora do przechowywania pewnych informacji w konkretnym państwie członkowskim) lub ograniczenia dotyczące swobodnego przepływu danych osobowych między państwami członkowskimi

[11] Art. 1 ust. 3 RODO.

(np. poprzez zawieszenie przepływu danych lub nałożenie tymczasowego lub całkowitego ograniczenia przetwarzania, w tym zakazu przetwarzania).

47. Podobnie swobodnemu przepływowi danych osobowych w Unii może zagrażać określanie oczekiwań (lub nakładanie wymogów) dotyczących sposobu, w jaki administratorzy wypełniają swoje obowiązki w ramach RODO, a mianowicie w taki sposób, że działania, których realizacji oczekuje się od administratorów, stają się powiązane z konkretnym regionem UE (np. poprzez szczegółowe wymogi dotyczące kwalifikacji).

48. Ponadto swobodny przepływ danych osobowych w Unii może również zostać utrudniony w razie wydania przez organy nadzorcze bezzasadnie odmiennych decyzji w sytuacjach, które są identyczne lub podobne (np. pod względem sektora lub rodzaju przetwarzania), ponieważ brak jednorodności zagrażałby równym warunkom działania w UE oraz prowadziłby do powstania w UE sytuacji, w których zachodzi sprzeczność, i wystąpienia ryzyka przemieszczania się pomiędzy jurysdykcjami ze względu na możliwość korzystniejszego rozstrzygnięcia sprawy (ang. *forum shopping)*. W tym względzie należy wziąć pod uwagę specyfikę krajową dopuszczoną w RODO w odniesieniu do niektórych sektorów takich jak opieka zdrowotna, dziennikarstwo lub archiwa.



Guidelines 8/2020 on the targeting of social media users

Version 2.0

Adopted on 13 April 2021

Version history

Version 2.0	13 April 2021	Adoption of the Guidelines after public consultation
Version 1.0	2 September 2020	Adoption of the Guidelines for publication consultation

TABLE OF CONTENTS

1 Introduction 4
2 Scope 5
3 Risks to the rights and freedoms of users posed by the processing of personal data 6
4 Actors and Roles 8
4.1 Users 8
4.2 Social media providers 9
4.3 Targeters 10
4.4 Other relevant actors 10
4.5 Roles and responsibilities 11
5 Analysis of different targeting mechanisms 13
5.1 Overview 13
5.2 Targeting on the basis of provided data 14
5.2.1 Data provided by the user to the social media provider 14
A. Roles 14
B. Legal basis 16
5.2.2 Data provided by the user of the social media platform to the targeter 18
A. Roles 19
B. Legal basis 20
5.3 Targeting on the basis of observed data 20
5.3.1 Roles 22
5.3.2 Legal basis 22
5.4 Targeting on the basis of inferred data 24
5.4.1 Roles 25
5.4.2 Legal basis 25
6 Transparency and right of access 26
6.1 Essence of the arrangement and information to provide (Article 26 (2) GDPR) 27
6.2 Right of access (Article 15) 28
7 Data protection impact assessments (DPIA) 30
8 Special categories of data 31
8.1 What constitutes a special category of data 31
8.1.1 Explicit special categories of data 32
8.1.2 Inferred and combined special categories of data 32
8.2 The Article 9(2) exception of special categories of data made manifestly public 34
9 Joint controllership and responsibility 36

9.1 Joint controller arrangement and determination of responsibilities (Art. 26 GDPR) 36
9.2 Levels of responsibility 38

The European Data Protection Board

Having regard to Article 70(1)(e) of Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

HAS ADOPTED THE FOLLOWING GUIDELINES

1 INTRODUCTION

1. A significant development in the online environment over the past decade has been the rise of social media. More and more individuals use social media to stay in touch with family and friends, to engage in professional networking or to connect around shared interests and ideas. For the purposes of these guidelines, social media are understood as online platforms that enable the development of networks and communities of users, among which information and content is shared.[1] Key characteristics of social media include the ability for individuals to register in order to create "accounts" or "profiles" for themselves, to interact with one another by sharing user-generated or other content and to develop connections and networks with other users.[2]

2. As part of their business model, many social media providers offer targeting services. Targeting services make it possible for natural or legal persons ("targeters") to communicate specific messages to the users of social media in order to advance commercial, political, or other interests.[3] A distinguishing characteristic of targeting is the perceived fit between the person or group being targeted and the message that is being delivered. The underlying assumption is that the better the fit, the higher the reception rate (conversion) and thus the more effective the targeting campaign (return on investment).

3. Mechanisms to target social media users have increased in sophistication over time. Organisations now have the ability to target individuals on the basis of a wide range of criteria. Such criteria may have been developed on the basis of personal data which users have actively provided or shared, such as their relationship status. Increasingly, however, targeting criteria are also developed on the basis of personal data which has been observed or inferred, either by the social media provider or by third parties, and collected (aggregated) by the platform or by other actors (e.g. data brokers) to support

[1] Additional functions provided by social media may include, for example, personalization, application integration, social plug-ins, user authentication, analytics and publishing. Social media functions may be a standalone offering of controllers or they may be integrated as part of a wider service offering.
[2] In addition to "traditional" social media platforms, other examples of social media include: dating platforms where registered users present themselves to find partners they can date in real life; platforms where registered users can upload their own videos, comment on and link to other's videos; or computer games where registered users may play together in groups, exchange information or share their experiences and successes within the game.
[3] Targeting has been defined as "the act of directing or aiming something at a particular group of people" and "the act of attempting to appeal to a person or group or to influence them in some way". https://www.collinsdictionary.com/dictionary/english/targeting.

ad-targeting options. In other words, the targeting of social media users involves not just the act of "selecting" the individuals or groups of individuals that are the intended recipients of a particular message (the 'target audience'), but rather it involves an entire process carried out by a set of stakeholders which results in the delivery of specific messages to individuals with social media accounts.[4]

4. The combination and analysis of data originating from different sources, together with the potentially sensitive nature of personal data processed in the context of social media[5], creates risks to the fundamental rights and freedoms of individuals. From a data protection perspective, many risks relate to the possible lack of transparency and user control. For the individuals concerned, the underlying processing of personal data which results in the delivery of a targeted message is often opaque. Moreover, it may involve unanticipated or undesired uses of personal data, which raise questions not only concerning data protection law, but also in relation to other fundamental rights and freedoms. Recently, social media targeting has gained increased public interest and regulatory scrutiny in the context of democratic decision making and electoral processes.[6]

2 SCOPE

5. Targeting of social media users may involve a variety of different actors which, for the purposes of these guidelines, shall be divided into four groups: social media providers, their users, targeters and other actors which may be involved in the targeting process. The importance of correctly identifying the roles and responsibilities of the various actors has recently been highlighted with the judgments in *Wirtschaftsakademie* and *Fashion ID* of the Court of Justice of the European Union (CJEU).[7] Both judgments demonstrate that the interaction between social media providers and other actors may give rise to joint responsibilities under EU data protection law.

6. Taking into account the case law of the CJEU, as well as the provisions of the GDPR regarding joint controllers and accountability, the present guidelines offer guidance concerning the targeting of social media users, in particular as regards the responsibilities of targeters and social media providers. Where joint responsibility exists, the guidelines will seek to clarify what the distribution of responsibilities might look like between targeters and social media providers on the basis of practical examples.[8]

7. The main aim of these guidelines is therefore to clarify the roles and responsibilities among the social media provider and the targeter. In order to do so, the guidelines also identify the potential risks for the rights and freedoms of individuals (section 3), the main actors and their roles (section 4), and tackle

[4] The messages delivered typically consist of images and text, but may also involve video and/or audio formats.
[5] Personal data processed in the context of social media may constitute 'special categories of personal data' pursuant to Article 9 GDPR, relate to vulnerable individuals, or otherwise be of a highly personal nature. See also Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP 248 rev. 01, p. 9.
[6] See, for example: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-03-13-statement-on-elections_en.pdf; https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/07/findings-recommendations-and-actions-from-ico-investigation-into-data-analytics-in-political-campaigns/; https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-data-protection-law-electoral-guidance-638_en.pdf; https://www.personuvernd.is/information-in-english/greinar/nr/2880.
[7] CJEU, Judgment in *Wirtschaftsakademie*, 5 June 2018, C-210/16, ECLI:EU:C:2018:388; CJEU, Judgment in *Fashion ID*, 29 July 2019, C-40/17, ECLI:EU:C:2019:629.
[8] The present guidance is without prejudice to the EDPB Guidelines 07/2020 on the concepts of controller and processor under the GDPR adopted on 02 September 2020, concerning the distribution of responsibilities in other contexts.

the application of key data protection requirements (such as lawfulness and transparency, DPIA, etc.) as well as key elements of arrangements between social media providers and the targeters.

8. Nevertheless, the scope of these Guidelines covers the relationships between the registered users of a social network, its providers, as well as the targeters. Thorough analysis, of scenarios, such as individuals that are not-registered with social media providers does not fall under the scope of the present guidelines.

3 RISKS TO THE RIGHTS AND FREEDOMS OF USERS POSED BY THE PROCESSING OF PERSONAL DATA

9. The GDPR underlines the importance of properly evaluating and mitigating any risks to the rights and freedoms of individuals resulting from the processing of personal data.[9] The mechanisms that can be used to target social media users, as well as the underlying processing activities that enable targeting, may pose significant risks. These guidelines do not seek to provide an exhaustive list of the possible risks to the rights and freedoms of individuals. Nonetheless, the EDPB considers it important to point out certain types of risks and to provide a number of examples how they may manifest themselves.

10. Targeting of social media users may involve uses of personal data that go against or beyond individuals' reasonable expectations and thereby infringes applicable data protection principles and rules. For example, where a social media platform combines personal data from third-party sources with data disclosed by the users of its platform, this may result in personal data being used beyond their initial purpose and in ways the individual could not reasonably anticipate. The profiling activities that are connected to targeting might involve an inference of interests or other characteristics, which the individual had not actively disclosed, thereby undermining the individual's ability to exercise control over his or her personal data.[10] Moreover, a lack of transparency regarding the role of the different actors and the processing operations involved may undermine, complicate or hinder the exercise of data subject rights.

11. A second type of risk concerns the possibility of discrimination and exclusion. Targeting of social media users may involve criteria that, directly or indirectly, have discriminatory effects relating to an individual's racial or ethnic origin, health status or sexual orientation, or other protected qualities of the individual concerned. For example, the use of such criteria in the context of advertising related to job offers, housing or credit (loans, mortgages) may reduce the visibility of opportunities to persons within certain groups of individuals. The potential for discrimination in targeting arises from the ability for advertisers to leverage the extensive quantity and variety of personal data (e.g. demographics, behavioral data and interests) that social media platforms gather about their users.[11] Recent research

[9] According to Article 24 of the GDPR, the controller shall implement appropriate technical and organizational measures to ensure and be able to demonstrate that processing is performed in accordance with the GDPR, "taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons". See also Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP248 rev. 01, 4 October 2017.
[10] See also European Data Protection Supervisor, EDPS Opinion on online manipulation, Opinion 3/2018, 19 March 2018, p. 15 ("*The concern of using data from profiles for different purposes through algorithms is that the data loses its original context. Repurposing of data is likely to affect a person's informational self-determination, further reduce the control of data subjects' over their data, thus affecting the trust in digital environments and services.*").
[11] T. Speicher a.o., Potential for Discrimination in Online Targeted Advertising, Proceedings of the 1st Conference on Fairness, Accountability and Transparency, *Proceedings of Machine Learning Research* PMLR 81:5-19, 2018, http://proceedings.mlr.press/v81/speicher18a.html.

suggests that the potential for discriminatory effects exists also without using criteria that are directly linked to special categories of personal data in the sense of Article 9 of the GDPR.[12]

12. A second category of risk relates to potential possible manipulation of users. Targeting mechanisms are, by definition, used in order to influence the behaviour and choices of individuals, whether it be in terms of their purchasing decisions as consumers or in terms of their political decisions as citizens engaged in civic life.[13] Certain targeting approaches may however go so far as to undermine individual autonomy and freedom (e.g. by delivering individualized messages designed to exploit or even accentuate certain vulnerabilities, personal values or concerns). For example, an analysis of content shared through social media can reveal information about the emotional state (e.g. through an analysis of the use of certain key words). Such information could be used to target the individual with specific messages and at specific moments to which he or she is expected to be more receptive, thereby surreptitiously influencing his or her thought process, emotions and behaviour.[14]

13. Mechanisms to target social media users can also be used to unduly influence individuals when it comes to political discourse and democratic electoral processes.[15] While 'traditional' offline political campaigning intends to influence voters' behaviour via messages that are generally available and retrievable (verifiable), the available online targeting mechanisms enable political parties and campaigns to target individual voters with tailored messages, specific to the particular needs, interests and values of the target audience.[16] Such targeting might even involve disinformation or messages that individuals find particularly distressing, and are therefore (more) likely to stimulate a certain emotion or reaction by them. When polarising or untruthful (disinformation) messages are targeted at specific individuals, with no or limited contextualisation or exposure to other viewpoints, the use of targeting mechanisms can have the effect of undermining the democratic electoral process.[17]

14. In the same vein, the use of algorithms to determine which information is displayed to which individuals may adversely affect the likelihood of access to diversified sources of information in relation to a particular subject matter. This may in turn have negative consequences for the pluralism of public debate and access to information.[18] Targeting mechanisms can be used to augment the visibility of certain messages, while giving less prominence to others. The potential adverse impact may be felt at two levels. On the one hand, there are risks related to so-called 'filter-bubbles' where people are exposed to 'more-of-the-same' information and encounter fewer opinions, resulting in increased political and ideological polarisation.[19] On the other hand, targeting mechanisms may also create risks

[12] Idem.
[13] European Data Protection Supervisor, Opinion 3/2018, p. 18.
[14] See 'Experimental evidence of massive-scale emotional contagion through social networks', Adam D. I. Kramer, Jamie E. Guillory, and Jeffrey T. Hancock, PNAS June 17, 2014 111 (24) 8788-8790; first published June 2, 2014 https://doi.org/10.1073/pnas.1320040111, available at: https://www.pnas.org/content/111/24/8788 Adam D. I. Kramer Core Data Science Team, Facebook, Inc., Menlo Park, CA 94025.
[15] See also European Data Protection Board, Statement 2/2019 on the use of personal data in the course of political campaigns, 13 March 2019, p. 1.
[16] Information Commissioner's Office (ICO), *Democracy disrupted? Personal information and political influence*, 10 July 2018, p. 14.
[17] See also European Commission, Commission Guidance on the application of Union data protection law in the electoral context, A contribution from the European Commission to the Leaders' meeting in Salzburg on 19-20 September 2018. See also L.M. Neudert and N.M. Marchal, Polarisation and the use of technology in political campaigns and communication, European Parliamentary Research Service, 2019, p. 22-24.
[18] See also European Parliament resolution of 3 May 2018 on media pluralism and media freedom in the European Union.
[19] European Data Protection Supervisor, Opinion 3/2018, p. 7.

of "information overload", whereby individuals cannot make an informed decision because they have too much information and cannot tell if it is reliable.

15. The collection of personal data by social media providers may not be limited to the activities performed by individuals on the social media platform itself. The targeting of social media users on the basis of information concerning their browsing behaviour or other activities outside the social media platform can give individuals the feeling that their behaviour is systematically being monitored. This may have a chilling effect on freedom of expression, including access to information.[20] Such effects may be exacerbated if targeting is also based on the analysis of content shared by social media users. If private messages, posts and comments are subject to analysis for commercial or political use, this may also give rise to self-censorship.

16. The potential adverse impact of targeting may be considerably greater where vulnerable categories of individuals are concerned, such as children. Targeting can influence the shaping of children's personal preferences and interests, ultimately affecting their autonomy and their right to development. Recital 38 of the GDPR indicates that specific protection should apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child.[21]

17. The use of social media in the EU is widespread as 54% of people aged 16-74 participated in social networks in 2019. Besides, this participation rate has steadily increased over the years.[22] The EDPB recognizes that the increase in concentration in the markets of social media and targeting may also increase risks to the rights and freedoms of a substantial number of individuals. For example, certain social media providers may be able to combine, either alone or in connection with other companies, a higher quantity and diversity of personal data. This ability, in turn, may increase the ability to offer more advanced targeting campaigns. This aspect is relevant from both a data protection (more in-depth profiling of the persons concerned) and competition law viewpoint (the unrivalled insight capabilities provided by the platform may make it an *'unavoidable trading partner'* for online marketers). The degree of market and informational power, in turn, as the EDPB has recognised, "*has the potential to threaten the level of data protection and freedom enjoyed by consumers of digital services*".[23]

18. The likelihood and severity of the aforementioned risks will depend, inter alia, on the nature of the targeting mechanism and how and for which exact purpose(s) it is used. Elements which may affect the likelihood and severity of risks in the context of the targeting of social media users will be discussed in greater detail in section 7.

4 ACTORS AND ROLES

4.1 Users

19. Individuals make use of social media in different capacities and for different purposes (e.g. to stay in touch with friends, to exchange information about shared interests, or to seek out employment

[20] European Data Protection Supervisor, Opinion 3/2018, p. 9 and Committee of experts on media pluralism and transparency of media ownership (MSI-MED), Internet and Electoral Campaigns, Study on the use of internet in electoral campaigns, Council of Europe study DGI(2017)11, April 2018, p. 19-21.
[21] See also Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 6 February 2018, WP251rev.01, p. 29.
[22] https://ec.europa.eu/eurostat/en/web/products-eurostat-news/-/edn-20200630-2.
[23] Statement of the EDPB on the data protection impacts of economic concentration, available at: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_economic_concentration_en.pdf

opportunities). The term "user" is typically used to refer to individuals who are registered with the service (i.e. those who have an "account" or "profile"). Many social media services can, however, also be accessed by individuals without having registered (i.e. without creating an account or profile).[24] Such individuals are typically not able to make use of all of the same features or services offered to individuals who have registered with the social media provider. Both individuals that are and that are not registered with the social media providers may be considered "data subjects" within the meaning of Article 4(1) GDPR insofar as the individual is directly or indirectly identified or identifiable.[25]

20. Whether or not individuals are expected to register with a real name or use a nickname or pseudonym may vary according to the social media service in question. It will generally still be possible, however, to target (or otherwise single out) the user in question even in the absence of a real name policy, as most types of targeting do not rely on user names but other types of personal data such as interests, sociographic data, behaviour or other identifiers. Social media providers often encourage their users to reveal "real world" data, such as telephone numbers.[26] Finally, it is worth noting that social media providers may also enable targeting of individuals who do not have an account with the social media provider.[27]

4.2 Social media providers

21. Social media providers offer an online service that enables the development of networks and communities of users, among which information and content is shared. Social media services are typically offered through web browsers or dedicated apps, often after having requested the user to provide a set of personal data to constitute the user's "account" or "profile". They also often offer users associated account "controls" to enable them to access and control the personal data processed in the context of the use of their account.

22. The social media provider determines the functionalities of the service. This in turn involves a determination of which data are processed, for which purpose, under which terms, as well as how personal data shall be processed. This allows for the provision of the social media service but also likely the provision of services, such as targeting, that can benefit business partners operating on the social media platform or in conjunction with it.

23. The social media provider has the opportunity to gather large amounts of personal data relating to users' and individuals' that are not registered with social media providers behaviour and interactions, which enables it to obtain considerable insights into the users' socio-demographic characteristics, interests and preferences. It is important to note that the 'insights' based on user activity often involve inferred or derived personal data. For example, where a user interacts with certain content (e.g. by "liking" a post on social media, or watching video content), this action can be recorded by the social media provider, and an inference might be made that the user in question enjoyed the content he or she interacted with.

[24] The personal data and profiling information maintained by social media providers in relation to individuals that are not registered with social media providers are sometimes referred to as "shadow profiles".
[25] See also recital (26) ("singling out"). See also Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, 20 June 2007, WP 136, p. 12 and following.
[26] In some cases, social media providers ask for additional documentation to further verify the data provided, for example by requesting users to upload their ID cards or similar documentation.
[27] Such targeting may be rendered possible on the basis of online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them. See also recital (30) GDPR.

24. Social media providers increasingly gather data not only from activities on the platform itself, but also from activities undertaken 'off-platform', combining data from multiple sources, online and offline, in order to generate further insights. The data can be combined with personal data that individuals actively disclose to the social media provider (e.g. a username, e-mail address, location, and phone number), alongside data which is "assigned" to them by the platform (such as unique identifiers).

4.3 Targeters

25. These guidelines use the term "targeter" to designate natural or legal persons that use social media services in order to direct specific messages at a set of social media users on the basis of specific parameters or criteria.[28] What sets targeters apart from other users of social media is that they select their messages and/or their intended audience according to the perceived characteristics, interests or preferences of the individuals concerned, a practice which is sometimes also referred to as "micro-targeting".[29] Targeters can engage in targeting to advance commercial, political, or other interests. Typical examples include brands who use social media to advertise their products including to increase brand awareness. Political parties also increasingly make use of social media as part of their campaigning strategy. Charities and other non-profit organisations also use social media to target messages at potential contributors or to develop communities.

26. It is important to note that social media users can be targeted in different ways. For example, targeting might occur not only through displaying personalized advertisement (e.g. through a "banner" shown on the top or side of a webpage), but - as far as it is happening within the social media platform - also through display in a user's "feed", "timeline" or "story", where the advertising content appears alongside user-generated content. Targeting may also involve the creation of content hosted by the social media provider (e.g. via a dedicated "page" or other social media presence) or elsewhere (i.e. on third-party websites). Targeters may have their own websites and apps, where they can integrate specific social media business tools or features such as social plugins or logins or by using the application programming interfaces (APIs) or software development kits (SDKs) offered by social media providers.

4.4 Other relevant actors

27. Targeters may directly use targeting mechanisms offered by social media providers or enlist the services of other actors, such as marketing service providers, ad networks, ad exchanges, demand-side and supply-side platforms, data management providers (DMPs) and data analytics companies. These actors are part of the complex and evolving online advertising ecosystem (which is sometimes known as "adtech") that collects and processes data relating to individuals (including social media users) by, for example, tracking their activities across websites and apps.[30]

28. Data brokers and data management providers are also relevant actors playing an important role in the targeting of social media users. Data brokers and DMPs differentiate themselves from other adtech companies to the extent that they not only process data collected by means of tracking technologies, but also by means of data collected from other sources, that can include both online and offline

[28] Processing of personal data by a natural person in the course of a purely personal or household activity does not fall under the material scope of the GDPR (Art. 2(2)(c)).
[29] Simply sharing information on a social media page which is intended for the public at large (e.g. information about opening hours) without prior selection of the intended audience would not be considered as «targeting» for the purposes of these guidelines.
[30] On the description of the different actors, see WP29, Opinion 2/2010 on behavioural advertisement, at page 5. The Opinion is available at:
https://ec.europa.eu/justice/Article-29/documentation/opinion-recommendation/files/2010/wp171_en.pdf

sources. In other words, data brokers and DMPs aggregate data collected from a wide variety of sources, which they then might sell to other stakeholders involved in the targeting process.[31]

29. While each of the other actors mentioned above can play an important role in targeting of social media users, the focus of the current guidelines is on the distribution of roles and data protection obligations of social media providers and targeters. Analogous considerations may apply, however, to the other actors involved in the online advertising ecosystem, depending on the role of each actor in the targeting process.

4.5 Roles and responsibilities

30. In order to clarify the respective roles and responsibilities of social media providers and targeters, it is important to take account of the relevant case law of the CJEU. The judgments in *Wirtschaftsakademie* (C-210/16), *Jehovah's Witnesses* (C-25/17) and *Fashion ID* (C-40/17) are particularly relevant here.

31. The starting point of the analysis is the legal definition of controller. According to Article 4(7) GDPR, a "'controller" means "*the natural or legal person [...] which, alone or jointly with others, determines the purposes and means of the processing of personal data*".

32. In *Wirtschaftsakademie*, the CJEU decided that the administrator of a so-called "fan page" on Facebook must be regarded as taking part in the determination of the purposes and means of the processing of personal data. According to the submissions made to the CJEU, the creation of a fan page involves the *definition of parameters* by the administrator, which has an *influence* on the processing of personal data for the purpose of *producing statistics* based on visits to the fan page.[32] Using the filters provided by Facebook, the administrator can define the criteria in accordance with which the statistics are to be drawn up, and even designate the categories of persons whose personal data is to be made use of by Facebook:

> *"In particular, the administrator of the fan page can ask for — and thereby request the processing of — demographic data relating to its target audience, including trends in terms of age, sex, relationship and occupation, information on the lifestyles and centers of interest of the target audience and information on the purchases and online purchasing habits of visitors to its page, the categories of goods and services that appeal the most, and geographical data which tell the fan page administrator where to make special offers and where to organise events, and more generally enable it to target best the information it offers."*

33. As the definition of parameters depends inter alia on the administrator's target audience "and the objectives of managing and promoting its activities", the administrator also participates in determining the purposes of the processing of personal data.33 The administrator was therefore categorised as a controller jointly responsible for the processing of personal data of the visitors of its 'page', together with the social media provider.

34. As further developed in section 9 of the present guidelines, controllers may be involved at different stages of the processing of personal data and to different degrees. In such circumstances, the level of responsibility of each of them must be assessed with regard to all the relevant circumstances of the particular case:

> *"[T]he existence of joint responsibility does not necessarily imply equal responsibility of the various operators involved in the processing of personal data. On the contrary, those operators may be involved at different stages of that processing of personal data and to different degrees, so that the level of responsibility of each of them must be assessed with regard to all the relevant circumstances of the particular case*."[34]

35. While concluding that the administrator of a page acts as a controller, jointly with Facebook, the CJEU also noted that in the present case, Facebook must be regarded as *primarily* determining the purposes and means of processing the personal data of users of Facebook and persons visiting the fan pages hosted on Facebook.[35]

36. In *Fashion ID*, the CJEU decided that a website operator can be a considered a controller when it embeds a Facebook social plugin on its website that causes the browser of a visitor to transmit personal data of the visitor to Facebook.[36] The qualification of the website operator as controller is, however, limited to the operation or set of operations in respect of which it actually determines the purposes and means. In this particular case, the CJEU considered that the website operator is only capable of determining, jointly with Facebook, the purposes and means of the collection and disclosure by transmission of the personal data of visitors to its website. As a result, the CJEU ruled that, for what concerns the embedding of a social plug-in within a website, the liability of the website operator is:

> *"limited to the operation or set of operations involving the processing of personal data in respect of which it actually determines the purposes and means, that is to say, the collection and disclosure by transmission of the data at issue."*[37]

37. The CJEU considered that the website operator was not a controller for subsequent38 operations involving the processing of personal data carried out by Facebook after their transmission to the latter, as the website operator was not in a position to determine the purposes and means of those operations by virtue of embedding the social plug-in:

> *"By contrast, in the light of that information, it seems, at the outset, impossible that Fashion ID determines the purposes and means of subsequent operations involving the processing of personal data carried out by Facebook Ireland after their transmission to the latter, meaning that Fashion ID cannot be considered to be a controller in respect of those operations [...]"*.[39]

38. In case of joint controllership, pursuant to Article 26(1) GDPR, controllers are required to put in place an arrangement which, in a transparent manner, determines their respective responsibilities for compliance with the GDPR, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14 GDPR.

---

[31] See Consumer Policy Research Centre, "*A day in the life of data*", available at: http://cprc.org.au/publication/research-report-a-day-in-the-life-of-data/
[32] Judgment in *Wirtschaftsakademie*, C-210/16, paragraph 36.
[33] Judgment in *Wirtschaftsakademie*, C-210/16, paragraph 39.

[34] Judgment in *Wirtschaftsakademie*, C-210/16, paragraph 43; Judgment in *Jehovah's Witnesses*, C-25/17, paragraph 66 and Judgment in *Fashion ID*, C-40/17, paragraph 70.
[35] Judgment in *Wirtschaftsakademie*, C-210/16, paragraph 30.
[36] Judgment in *Fashion ID*, C-40/17, paragraph 75 and following and paragraph 107.
[37] Judgment in *Fashion ID*, C-40/17, paragraph 107.
[38] Subsequent processing is any processing operation or set of processing operations which follows (i.e. takes place after) the data collection. In Fashion ID, the term is used to refer to processing operations carried out by Facebook after their transmission and for which Fashion ID should not be considered as a joint controller (because it does not effectively participate in determining the purposes and means of those processing).
Subsequent processing for a purpose other than that for which the personal data have been collected is only permissible insofar as Article 6(4) GDPR relating to further processing is complied with. For example, if an online retailer collects data relating to an individual's home address, a subsequent processing would consist in the storage or later deletion of this information. However, if this online retailer later decides to process this personal data to enrich the profile of the data subject for targeting purposes, this would amount to further processing within the meaning of Article 6(4) GDPR as it involves processing for a purpose other than that for which they were initially collected.
[39] Judgment in *Fashion ID*, C-40/17, paragraph 76.

39. The following sections clarify, by way of specific examples, the roles of targeters and social media providers in relation to different targeting mechanisms. Specific considerations are given in particular as to how the requirements of lawfulness and purpose limitation apply in this context. Next, the requirements concerning transparency, data protection impact assessments and the processing of special categories of data are analysed. Finally, the Guidelines address the obligation for joint controllers to put in place an appropriate arrangement pursuant to Article 26 GDPR, taking into account the degree of responsibility of the targeter and of the social media provider.

5 ANALYSIS OF DIFFERENT TARGETING MECHANISMS

5.1 Overview

40. Social media users may be targeted on the basis of provided, observed or inferred data, as well as a combination thereof:

a) **Targeting individuals on the basis of provided data** – "Provided data" refers to information actively provided by the data subject to the social media provider and/or the targeter.[40] For example:

- A social media user might indicate his or her age in the description of his or her user profile. The social media provider, in turn, might enable targeting on the basis of this criterion.
- A targeter might use information provided by the data subject to the targeter in order to target that individual specifically, for example by means of customer data (such as an e-mail address list), to be matched with data already held on the social media platform, leading to all those users who match being targeted with advertising[41].

b) **Targeting on the basis of observed data** – Targeting of social media users can also take place on the basis of observed data.[42] Observed data are data provided by the data subject by virtue of using a service or device.[43] For example, a particular social media user might be targeted on the basis of:

- his or her activity on the social media platform itself (for instance the content that the user has shared, consulted or liked);
- the use of devices on which the social media's application is executed (for instance GPS coordinates, mobile telephone number);
- data obtained by a third-party application developer by using the application programming interfaces (APIs) or software development kits (SDKs) offered by social media providers;

[40] Article 29 Data Protection Working Party, Guidelines on the right to data portability, WP 242 rev.01, 5 April 2017, p. 10.
[41] See for example the decision by the Higher Administrative Court of Bavaria h (Germany), Beschluss v.26.09.2018 – 5 CS 18.1157, www.gesetze-bayern.de/Content/Document/Y-300-Z-BECKRS-B-2018-N-25018.
[42] In its Opinion 2/2010 on online behavioural advertising the WP29 noted that "*there are two main approaches to building user profiles: i) Predictive profiles are established by inference from observing individual and collective user behaviour over time, particularly by monitoring visited pages and ads viewed or clicked on. ii) Explicit profiles are created from personal data that data subjects themselves provide to a web service, such as by registering*" (Article 29 Data Protection Working Party, Opinion 2/2010 on online behavioural advertising, WP 171, p. 7).
[43] Article 29 Data Protection Working Party, Guidelines on the right to data portability, WP 242 rev.01, 5 April 2017, p. 10.

- data collected through third-party websites that have incorporated social plugins or pixels;
- data collected through other third parties (e.g. parties with whom the data subject has interacted, purchased a product, subscribed to loyalty cards); or
- data collected through services offered by companies owned or operated by the social media provider.

c) **Targeting on the basis of inferred data** – "Inferred data" or "derived data" are created by the data controller on the basis of the data provided by the data subject or as observed by the controller.[44] For example, a social media provider or a targeter might infer that an individual is likely to be interested in a certain activity or product on the basis of his or her web browsing behaviour and/or network connections.

5.2 Targeting on the basis of provided data

5.2.1 Data provided by the user to the social media provider

41. Individuals may actively disclose a great deal of information about themselves when making use of social media. The creation of a social media account (or "profile") involves disclosure of a number of attributes, which may include name, date of birth, gender, place of residence, language, etc. Depending on the nature of the social media platform, users may include additional information such as relationship status, interests or current employment. Personal data provided by social media users can be used by the social media provider to develop criteria, which enables the targeter to address specific messages at the users of the social media.

> Example 1:
>
> Company X sells gentlemen's shoes and wishes to promote a sale of its winter collection. For its advertising campaign, it wishes to target men between the age of 30 and 45 who have indicated that they are single in their social media profile. It uses the corresponding targeting criteria offered by the social media provider as parameters to identify the target audience to whom its advertisement should be displayed. Moreover, the targeter indicates that the advertisement should be displayed to social media users while they are using the social media service between the hours of 5pm and 8pm. To enable targeting of social media users on the basis of specific criteria, the social media provider has previously determined which types of personal data shall be used in order to develop the targeting criteria and which targeting criteria shall be offered. The social media provider also communicates certain statistical information once the advertisements has been displayed to the targeter (e.g. to report on the demographic composition of individuals that interacted with the advertisement).

A. Roles

42. In Example 1, both the targeter and the social media provider participate in determining the purpose and means of the processing personal data. This results in the display of the advertisement to the target audience.

43. As far as the determination of *purpose* is concerned, Company X and the social media provider jointly determine the purpose of the processing, which is to display a specific advertisement to a set of individuals (in this case social media users) who make up the target audience, by choosing available targeting criteria associated with these users in order to reach a likely interested audience and to

[44] *Idem.*

provide them more relevant advertisement content. Moreover, there is also mutual benefit arising from the same processing operation, which is an additional indicator that the purposes pursued by given Company X and the social media provider are inextricably be linked.[45]

44. As far as the determination of *means* is concerned, the targeter and the social media provider jointly determine the means, which results in the targeting. The targeter participates in the determination of the means by choosing to use the services offered by the social media provider[46], and by requesting it to target an audience based on certain criteria (i.e. age range, relationship status, timing of display).[47] In doing so, the targeter defines the criteria in accordance with which the targeting takes place and designates the categories of persons whose personal data is to be made use of. The social media provider, on the other hand, has decided to process personal data of its users in such a manner to develop the targeting criteria, which it makes available to the targeter.[48] In order to do so, the social media provider has made certain decisions regarding the essential means of the processing, such as which categories of data shall be processed, which targeting criteria shall be offered and who shall have access (to what types of) personal data that is processed in the context of a particular targeting campaign.[49]

45. For the sake of completeness, the EDPB notes that the social media provider does not qualify as a processor as defined in Article 4 (8) GDPR.[50] In Example 1, the targeting criteria, as developed by the social media provider on the basis of user's' personal data can be used by the social media provider for future processing operations, which demonstrates that the later cannot qualify as a processor. Moreover, the social media provider does not appear to exclusively process the data on behalf of Company X and in accordance with its instructions.

46. The joint control among the targeter and social media provider only extends to those processing operations for which they effectively co-determine the purposes and means. It extends to the processing of personal data resulting from the selection of the relevant targeting criteria and the display of the advertisement to the target audience. It also covers the processing of personal data undertaken by the social media provider to report to the targeter about the results of the targeting campaign. The joint control does not, however, extend to operations involving the processing of personal data at other stages occurring before the selection of the relevant targeting criteria or after the targeting and reporting has been completed (e.g. the development of new targeting criteria by the social media provider on the basis of completed targeting campaigns) and in which the targeter has

[45] See EDPB Guidelines 7/2020 on concepts of the controller and the processor in the GDPR, ("*In addition, when the entities do not have the same purpose for the processing, joint controllership may also, in light of the CJEU case law, be established when the entities involved pursue purposes which are closely linked or complementary. Such may be the case, for example, when there is a mutual benefit arising from the same processing operation, provided that each of the entities involved participates in the determination of the purposes and means of the relevant processing operation*").

[46] See EDPB Guidelines 7/2020 on concepts of the controller and the processor in the GDPR, ("*Furthermore, the choice made by an entity to use for its own purposes a tool or other system developed by another entity, allowing the processing of personal data, will likely amount to a joint decision on the means of that processing by those entities. This follows from the Fashion ID case where the CJEU concluded, that by embedding on its website the Facebook Like button made available by Facebook to website operators, Fashion ID has exerted a decisive influence in respect of the operations involving the collection and transmission of the personal data of the visitors of its website to Facebook and had thus jointly determined with Facebook the means of that processing*").

[47] See in this respect *Wirtschaftsakademie*, C-210/16, para. 39 - ECLI:EU:C:2018:388.

[48] See in the same vein also *Fashion ID*, C-40/17, para. 80: "*those processing operations are performed in the economic interests of both Fashion ID and Facebook Ireland, for whom the fact that it can use those data for its own commercial purposes is the consideration for the benefit to Fashion ID*".

[49] See Opinion 1/2010.

[50] See EDPB Guidelines 7/2020 on concepts of the controller and the processor in the GDPR.

not participated in determining the purposes and means, likewise the social media provider, in principle, does not participate in phase of planning a targeting campaign prior to the moment where the targeter makes contact with the social media provider".[51]

47. The above analysis remains the same even if the targeter only specifies the parameters of its intended audience and does not have access to the personal data of the users that are affected. Indeed, joint responsibility of several actors for the same processing does not require each of them to have access to the personal data concerned.[52] The EDPB recalls that actual access to personal data is not a prerequisite for joint responsibility.[53]

B. Legal basis

48. As joint controllers, both parties (the social media provider and the targeter) must be able to demonstrate the existence of a legal basis (Article 6 GDPR) to justify the processing of personal data for which each of the joint controllers is responsible. The EDPB recalls that no specific hierarchy is made between the different lawful basis of the GDPR: the controller needs to ensure that the selected lawful basis matches the objective and context of the processing operation in question. The identification of the appropriate lawful basis is tied to principles of fairness and purpose limitation.[54]

49. Generally speaking, there are two legal bases which could justify the processing that supports the targeting of social media users: data subject's consent (Article 6(1)(a) GDPR) or legitimate interests (Article 6(1)(f) GDPR). A controller must always consider what the appropriate legal basis is under the given circumstances. In respect to the social media providers Article 6 (1) b GDPR cannot provide a lawful basis for online advertising simply because such advertising indirectly funds the provision of their service. [55] The same applies to the targeter as targeting of social media users cannot be considered as an intrinsic aspect of any services or necessary to perform a contract with the user.[56] While personalisation of content may, in certain circumstances, constitute an intrinsic and expected element of certain online services[57], Article 6 (1) b GDPR in the context of targeting of social media users is hardly applicable, as illustrated in the examples of these Guidelines.[58]

[51] See also Judgment in *Fashion ID*, C-40/17, para. 74 ("*[a] natural or legal person cannot be considered to be a controller, within the meaning of that provision, in the context of operations that precede or are subsequent in the overall chain of processing for which that person does not determine either the purposes or the means*") and paragraph 101.

[52] Judgment in *Wirtschaftsakademie*, C-210/16, para. 38 - ECLI:EU:C:2018:388; Judgment in *Jehovah's Witnesses*, C-25/17, para. 69 - ECLI:EU:C:2018:551.

[53] CJEU Judgment 10 July 2018 (C-25/17, para. 68 to 72).

[54] See paragraph 18, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0, 8 October 2019, available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf

[55] See para. 52, 53, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0, 8 October 2019, available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf

[56] There would be a lack of necessity if the targeter were to switch to social media providers despite a direct contractual relationship with its customer and thus the possibility of direct advertising.

[57] See p. 15 , Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0, 8 October 2019, available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf

[58] Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, para 57.

50. For what concerns the legitimate interest lawful basis, the EDPB recalls that in *Fashion ID*, the CJEU reiterated that in order for a processing to rely on the legitimate interest, three cumulative conditions should be met, namely[59] (i) the pursuit of a legitimate interest by the data controller or by the third party or parties to whom the data are disclosed, (ii) the need to process personal data for the purposes of the legitimate interests pursued, and (iii) the condition that the fundamental rights and freedoms of the data subject whose data require protection do not take precedence. The CJEU also specified that in a situation of joint controllership "*it is necessary that each of those controllers should pursue a legitimate interest [...] through those processing operations in order for those operations to be justified in respect of each of them*".[60]

51. With regard to Example 1, the targeter might consider its legitimate interest to be the economic interest of having an increased publicity for its goods through social media targeting. The social media provider could consider that its legitimate interest consists of making the social media service profitable by selling advertising space. Whether the targeter and the social media provider can rely upon Article 6(1)(f) GDPR as legal basis depends on whether all three cumulative conditions are met, as recently reiterated by the CJEU. Even if the targeter and the social media provider consider their economic interests to be legitimate, it does not necessarily mean that they will be able to actually rely on Article 6(1)(f) GDPR.

52. The second part of the balancing test entails that the joint controllers will need to establish that the processing is necessary to achieve those legitimate interests. "Necessary" requires a connection between the processing and the interests pursued. The 'necessity' requirement is particularly relevant in the context of the application of Article 6(1)f, in order to ensure that processing of data based on legitimate interests does not lead to an unduly broad interpretation of the necessity to process data. As in other cases, this means that it should be considered whether other less invasive means are available to serve the same end.[61]

53. The third step in assessing whether the targeter and the social media provider can rely upon Article 6(1)(f) GDPR as legal basis for the processing of personal data, is the balancing exercise necessary to determine whether the legitimate interest at stake is overridden by the data subject's interests or fundamental rights and freedoms.[62]

54. The EDPB recalls that in cases where a controller envisages to rely on legitimate interest, the duties of transparency and the right to object require careful consideration. Data subjects should be given the opportunity to object to the processing of their data for targeted purposes before the processing is initiated. Users of social media should not only be provided with the possibility to object to the display of targeted advertising when accessing the platform, but also be provided with controls that ensure the underlying processing of his or her personal data for the targeting purpose no longer takes place after he or she has objected.

55. The targeter seeking to rely on legitimate interest should, for its part, make it easy for individuals to express a prior objection to its use of social media for targeting purposes. However, insofar as the targeter does not have any direct interaction with the data subject, the targeter should at least ensure that the social media platform provide the data subject with means to efficiently express their right to prior objection. As joint controllers, the targeter and social media provider should clarify how the individuals' right to object (as well as other rights) will be accommodated in the context of the joint arrangement (see section 6). If the balancing exercise points out that data subject's interests or fundamental rights and freedoms override the legitimate interest of the social media provider and the targeter, the use of Article 6(1)(f) is not possible.

56. For what concerns the consent lawful basis, the controller needs to keep in mind that there are clearly situations in which the processing would not be lawful without the valid consent of the individuals concerned (Article 6(1)(a) GDPR). For example, the WP29 has previously considered that it would be difficult for controllers to justify using legitimate interests as a legal basis for intrusive profiling and tracking practices for marketing or advertising purposes, for example those that involve tracking individuals across multiple websites, locations, devices, services or data-brokering.[63]

57. To be valid, the consent collected for the processing needs to fulfil the conditions laid out in Articles 4(11) and 7 GDPR. Generally speaking, consent can only be an appropriate legal basis if a data subject is offered control and genuine choice. If consent is bundled up as a non-negotiable part of terms and conditions, it is presumed not to have been freely given. Consent must also be specific, informed and unambiguous and the data subject must be able to refuse or withdraw consent without detriment.[64]

58. Consent (Article 6(1)(a) GDPR) could be envisaged, provided that all the requirements for valid consent are met. The EDPB recalls that obtaining consent also does not negate or in any way diminish the controller's obligations to observe the principles of processing enshrined in the GDPR, especially Article 5 with regard to fairness, necessity and proportionality, as well as data quality. Even if the processing of personal data is based on consent of the data subject, this would not legitimize targeting which is disproportionate or unfair.[65]

59. Finally, the EDPB is of the opinion that the processing of personal data described in the Example 1 cannot be justified on the basis of Article 6(1)(b) by neither the social platform nor the targeter.[66]

5.2.2 Data provided by the user of the social media platform to the targeter

60. Targeting can also involve data provided by the data subject to the targeter, who then uses the data collected in order to target the data subject on social media. For example, "list-based" targeting occurs where a targeter uploads pre-existing lists of personal data (such as e-mail addresses or phone numbers) for the social media provider to match against the information on the platform. In this case,

[59] CJEU, Judgment in *Fashion ID*, 29 July 2019, C-40/17, para. 95 - ECLI:EU:C:2019:629.
[60] Idem, para 97.
[61] Article 29 Working Party Opinion 06/2014 on the concept of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP217, 9 April 2014, p. 29.
[62] When assessing the impact on the interests, fundamental rights and freedoms of the individual concerned, the following considerations are particularly relevant in the context of targeting directed to users of social media (i) the purposes of the targeting, (ii) the level of detail of the targeting criteria used (e.g., a broadly described cohort such as 'people with an interest in English literature', or more detailed criteria to allow segmentation and targeting on a more granular level), (iii) the type (and combination) of targeting criteria used (i.e. whether the targeting only focuses on a small aspect of the data subject, or is more comprehensive in nature), and (iv) the nature (sensitivity), volume and source of the data used in order to develop the targeting criteria. See Article 29 Working Party Opinion 06/2014 on the concept of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP217, 9 April 2014 https://ec.europa.eu/justice/Article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf

[63] Article 29 Working Party, Opinion on profiling and automated decision making, WP 251, rev. 01, p. 15, see also Article 29 WP, Opinion on legitimate interest, p. 32 and 48: « Overall, there is an imbalance between the company's legitimate interest and the protection of users' fundamental rights and Article 7(f) should not be relied on as a legal ground for processing. Article 7(a) would be a more appropriate ground to be used, provided that the conditions for a valid consent are met ».
[64] See Article 29 Working Party, Guidelines on consent under Regulation 2016/679, WP259 rev.01.
[65] See Article 29 Working Party, Guidelines on consent under Regulation 2016/679, WP259 rev.01, p. 3-4.
[66] See Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0, 8 October 2019, available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf

the social media provider compares the data uploaded by the targeter with user data that it already possesses, and any users that match are added to or excluded from the target audience (that is, the 'cluster' of persons to which the advertisement will be displayed on the social media platform). The social media provider may also allow the targeter to 'check' the list prior to finalising it, meaning that some processing takes place even before the audience has been created.

Example 2:

Ms. Jones contacts Bank X to set up an appointment regarding a possible mortgage because she is buying a house. She contacts the bank via e-mail to set up the appointment. Following the appointment, Ms. Jones decides not to become a customer of the bank. The bank has nevertheless added the e-mail address of Ms. Jones to its customer e-mail database. Then, the bank uses its e-mail database, by allowing the social media provider to 'matching' the list of e-mail addresses it holds with those held by the social media platform, in order to target the individuals concerned with the full range of financial services on the social media platform.

Example 3:

Mr. Lopez has been a customer at Bank X for almost a year. When he became a customer, he provided an e-mail address and was informed by Bank X, at the moment of collection, that: (a) his e-mail address would be used for advertising of offers linked to the bank services that he is already using; and (b) he may object to this processing at any time. The bank has added his e-mail address to its customer e-mail database. Afterwards, the bank uses its e-mail database to target its customers on the social media platform with the full range of financial services it has on offer.[67]

A. Roles

61. In these examples, the targeter, i.e. the bank, acts as a controller because it determines the purposes and means of the processing by actively collecting, processing and transmitting the personal data of the individuals concerned to the social media provider for advertising purposes. The social media provider, in turn, acts as a controller because it has taken the decision to use personal data acquired from the social media user (i.e. the e-mail address provided when setting up his or her account) in order to enable the targeter to display advertising to an audience of specific individuals.

62. Joint controllership exists in relation to the processing operations for which the social media provider and the targeter jointly determine the purposes and means, in this case, uploading unique identifiers related to the intended audience, matching, selection of targeting criteria and subsequent display of the advertisement, as well as any reporting relating to the targeting campaign.[68]

[67] In situations where e-mail addresses are used to send direct marketing to users controllers must also take into account the provisions of Article 13 of the ePrivacy Directive. ".

[68] The determination of purposes and means of the processing of the targeter and social media provider is similar (albeit not identical) to Example 1. By uploading the list of email addresses and setting the additional targeting criteria, the targeter defines the criteria in accordance with which the targeting takes place and designates the categories of persons whose personal data is to be made use of. The social media provider likewise makes a determination as to whose personal data shall be processed, by allowing which categories of data shall be processed, which targeting criteria shall be offered and who shall have access (to what types of) personal data that is processed in the context of a particular targeting campaign. The shared purpose underlying these processing operations resembles the purpose identified in Example 1, namely the display a specific advertisement to a set of individuals (in this case: social media users) who make up the target audience.

63. In both examples the bank acts as the sole controller regarding the initial collection of the email addresses of Ms. Jones and Mr. Lopez respectively. The social media provider does not participate in any way to determine the means and purposes of this collection. The joint control begins with the transmission of the personal data and the simultaneous collection of it by the social media provider. It continues throughout the display of the targeted advertisement ends (in most of the cases) when a subsequent reporting phase is completed. In some cases, joint controllership can be further extended, even until the deletion of the data phase insofar as the targeter still continues to participate in the determination of purposes and means.

64. The reason why the bank acts as sole controller when collecting the e-mail addresses from Ms. Jones and Mr. Lopez respectively, is because the collection of data occurs prior to (and is not inextricably linked to) the targeting campaign. Therefore, in this case one must distinguish between the initial set of processing operations for which only the bank is a controller and a subsequent processing for which joint control exists. The responsibility of the bank does not extend to operations occurring after the targeting and reporting has been completed and in which the targeter has not participated in the purposes and means and for which the social media provider acts as the sole controller.

B. Legal basis

65. In Example 2, Article 6(1)f GDPR does not provide an appropriate legal basis to justify the processing in this case, taking into account the context in which the personal data was provided. Indeed, Ms. Jones contacted the bank for the sole purpose of setting up an appointment, following which she communicated her intention not to make use of the services offered by the bank. Hence, one can consider that there is no reasonable expectation by Ms. Jones that her personal data shall be used for targeting purposes ('re-targeting'). Moreover, a compatibility test under Article 6(4) GDPR would likely lead to the outcome that this processing is not compatible with the purpose for which the personal data are initially collected.

66. In Example 3, the targeter might be able to rely on legitimate interest to justify the processing, taking into account inter alia that Mr. Lopez was: (a) informed of the fact that his e-mail address may be used for purposes of advertising via social media for services linked to the one used by the data subject; (b) the advertisement relates to services similar to those for Mr. Lopez is already a customer, and (c) Mr. Lopez was given the ability to object prior to the processing, at the moment where the personal data were collected by the bank. However, the EDPB would like to clarify that the fulfillment of information duties as per Articles 13 and 14 GDPR and the weighing of interests to be performed according to Article 6 (1)(f) GDPR are two different sets of obligations. Therefore, the mere fulfilment of information duties according to Articles 13 and 14 GDPR is not a transparency measure to be taken into consideration for the weighing of interests according to Article 6 (1)(f) of GDPR.

5.3 Targeting on the basis of observed data

67. There are several ways in which social media providers may be able to observe the behaviour of their users. For example, observation is possible through the social media service itself or may also be possible on external websites by virtue of social plug-ins or pixels.

Example 4: Pixel-based targeting

Mr Schmidt is browsing online in order to purchase a backpack. He visits the website "BestBags.com", views a number of items, but decides not to make a purchase. The operator of "BestBags.com" wishes to target social media users who have visited their website without making a purchase. To this end, it

integrates a so-called "tracking pixel"[69] on its website, which is made available by the social media provider. After leaving the website of BestBags.com and logging into his social media account, Mr Schmidt begins to see advertisement for the backpacks he was considering when browsing BestBags.com.

Example 5: Geo-targeting

Mrs Michu has installed the application of a social media provider on her smartphone. She is walking around Paris during her holidays. The social media provider collects information regarding Mrs Michu's whereabouts via the GPS functionalities of her smartphone on an ongoing basis[70], using the permissions that have been granted to the social media provider when the application was installed. Mrs Michu is staying at a hotel that is located next to a pizzeria. The pizzeria uses the geo-targeting functionality offered by the social media provider to target individuals who are within 1km of its premises for the first time in the last 6 months. When opening the social media provider's application on her smartphone, Mrs Michu sees an advertisement from the pizzeria, decides that she is hungry and buys a pizza via its website.

Example 6:

Mrs Ghorbani creates an account on a social media platform. During the process of registration she is asked if she consents to the processing of her personal data to see targeted advertisement on her social media page, on the basis of data she directly provides to the social media provider (such as her age, sex and location), as well as on the basis of her activity on other websites outside of the social media platform using cookies. She is informed that this data will be collected via social media plug-ins or tracking pixels, the processes are clearly described to her, as well as the fact that targeting involves other entities who are jointly responsible for ensuring compliance with the GDPR. It is also explained to her that she can withdraw her consent at any time, and she is provided with a link to the privacy policy. Because Mrs Ghorbani is interested in seeing targeted advertisement on her social media page, she gives her consent. No advertising cookies are placed or collected until Mrs Ghorbani expresses here consent.

Later on, she visits the website "Thelatesthotnews.com" that has a social media button integrated on it. A small but clearly visible banner appears on the right edge of the screen, asking Mrs Ghorbani to consent to the transmission of her personal data to the social media provider using cookies and social media plug-ins. The website operator undertook technical measures so that no personal data is transferred to the social media platform until she gives her consent.

[69] Tracking pixels are comprised of small snippets of code that are integrated into the website of the targeter. When an individual accesses the targeter's website in their browser, the browser automatically sends a request to the social media provider's server to obtain the tracking pixel. Once the tracking pixel is downloaded, the social media provider is typically able to monitor the user's session (i.e. the individual's behaviour on the website(s) in question). The observed data can be used in order for example to add a social media user to a particular target audience.

[70] A social media provider may also be able to determine the whereabouts of their users on the basis of other data points, including IP address and WiFi information from mobile devices, or the user-derived data (e.g. if they place information about their location on the platform in a post).

5.3.1 Roles

68. In Example 4, both the targeter and the social media provider participate in determining the purposes and means of the processing of personal data, which results in the display of the advertisement to Mr. Schmidt.

69. As far as the determination of purpose is concerned, Bestbags.com and the social media provider jointly determine the purpose of the processing, which is to display a specific advertisement on the social media platform to the individuals who make up the target audience. By embedding the pixel into its website, Bestbags.com exerts a decisive influence over the means of the processing. The collection and transmission of the personal data of visitors of the website to the social media provider would not have occurred without the embedding of that pixel. The social media provider, on the other hand, has developed and offers the software code (pixel) that leads to the automatic collection, transmission and evaluation for marketing purposes of personal data to the social media provider. As a result, joint controllership exists in relation to the collection of personal data and its transmission by way of pixels, as well as in relation to the matching and subsequent display of the advertisement to Mr Schmidt on the social platform, and for any reporting relating to the targeting campaign. Joint controllership also exists, for similar reasons, in Example 6.

70. In Example 5, the pizzeria exercises a decisive influence over the processing of personal data by defining the parameters of the ad targeting in accordance with its business needs (for instance, opening hours of the pizzeria and geo-location of persons close to the pizzeria in this time-slot), and therefore must be regarded as taking part in the determination of the purposes and means of the data processing. The social media provider, on the other hand, has collected the information regarding Mrs. Michu's location (via GPS) for its purpose of enabling such location-based targeted advertising. As a result, joint control exists between the targeter and the social platform in relation to the collection and analysis of Mrs. Michu's location, as well as the display of the advertisement, in order to target her (as a person appearing within 1km of the pizzeria for the first time in the last 6 months) with the ad.

5.3.2 Legal basis

71. First of all, because Examples 4, 5 and 6 involve the use of cookies, requirements resulting from Article 5(3) of the ePrivacy Directive need to be taken into account.

72. In this regard, it should be noted that Article 5(3) of the ePrivacy Directive requires that users are provided with clear and comprehensive information, inter alia about the purposes of the processing, prior to giving their consent[71], subject to very narrow exceptions.[72] Clear and comprehensive information implies that a user is in a position to be able to determine easily the consequences of any consent he or she might give and ensure that the consent given is well informed.[73] As a result, the controller will have to inform data subjects about all the relevant purposes of the processing – including any subsequent processing of the personal data obtained by accessing information in the terminal equipment.

73. To be valid, the consent collected for the implementation of tracking technologies needs to fulfil the conditions laid out in Article 7 GDPR.[74] For instance, consent is not validly constituted if the use of cookies is permitted by way of a checkbox pre-ticked by the service provider, which the user must

[71] Court of Justice of the European Union, Judgment in Planet 49 Gmbh, Case C-673/17, paragraph 73.

[72] See Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities. See also Court of Justice of the European Union, Judgment in Fashion ID, C-40/17, paragraphs 89-91.

[73] *Idem*, paragraph 74.

[74] EDPB Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.1, p. 6.

deselect to refuse his or her consent.[75] Based on recital 32, actions such as scrolling or swiping through a webpage or similar user activity will not under any circumstances satisfy the requirement of a clear and affirmative action: such actions may be difficult to distinguish from other activity or interaction by a user and therefore determining that an unambiguous consent has been obtained will also not be possible. Furthermore, in such a case, it will be difficult to provide a way for the user to withdraw consent in a manner that is as easy as granting it.[76]

74. Any (joint) controller seeking to rely on consent as a legal basis is responsible for ensuring that valid consent is obtained. In *Fashion ID*, the CJEU emphasized the importance of ensuring the efficient and timely protection of the data subject rights, and that consent should not be given only to the joint controller that is involved later in the processing. Valid consent must be obtained prior to the processing, which implies that (joint) controllers need to assess when and how information should be provided and consent should be obtained. In other words, the question as to which of the joint controllers should be in charge of collecting the consent comes down to determining which of them is involved first with the data subject. In example 6, as the placement of cookies and processing of personal data occurs at the moment of account creation, the social media provider must collect her valid consent before the placement of advertisement cookies.

75. The EDPB also recalls that in a case where the consent sought is to be relied upon by multiple (joint) controllers or if the data is to be transferred to or processed by other controllers who wish to rely on the original consent, these organisations should all be named.[77] Insofar as not all joint controllers are known at the moment when the social media provider seeks the consent, the latter will necessarily need to be complemented by further information and consent collected by the website operator embedding the social media plugin (i.e. *Thelatesthotnews.com* in Example 6).

76. The EDPB emphasizes that the consent that should be collected by the website operator for the transmission of personal data triggered by its website (by embedding a social plug-in) relates only to the operation or set of operations involving the processing of personal data in respect of which the operator actually determines the purposes and means[78]. The collection of consent by a website operator, i.e. "Thelatesthotnews.com" in Example 6 for instance, does not negate or in any way diminish the obligation of the social media provider to ensure the data subject has provided a valid consent for the processing for which it is responsible as a joint controller[79], as well as for any subsequent or further processing it carries out for which the website operator does not jointly determine the purposes and means (e.g. subsequent profiling operations for targeting purposes).

77. In addition, any subsequent processing of personal data, including personal data obtained by cookies, social plug-ins or pixels, must also have a legal basis under Article 6 of the GDPR in order to be lawful.[80] For what concerns the legal basis of the processing in Examples 4, 5, and 6, the EDPB considers that

[75] Court of Justice of the European Union, Judgement in Planet 49, C-637/17, paragraph 57.
[76] EDPB Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.1, p. 19.
[77] EDPB Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.1, p. 16, paragraph 65.
[78] Judgment in *Fashion ID*, 29 July 2019, C-40/17, ECLI:EU:C:2019:629, paragraphs 100-101.
[79] This is all the more the case insofar as that for most targeting tools, it is the social media that carries out the read/write operations on the terminal of the user, because it collects the personal data for the purpose of targeted advertisement. Therefore, the social media provider is responsible for ensuring that valid consent is obtained.
[80] Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities, paragraph 41.

legitimate interest cannot act as an appropriate legal basis, as the targeting relies on the monitoring of individuals' behaviour across websites and locations using tracking technologies.[81]

78. Therefore, in such circumstances, the appropriate legal basis for any subsequent processing under Article 6 GDPR is also likely to be the consent of the data subject. Indeed, when assessing compliance with Article 6 GDPR, one should take into account that the processing as a whole involves specific activities for which the EU legislature has sought to provide additional protection.[82] Moreover, controllers must take into account the impact on data subjects' rights when identifying the appropriate legal basis in order to respect the principle of fairness.[83]

5.4 Targeting on the basis of inferred data

79. Inferred data refers to data which is created by the controller on the basis of the data provided by the data subject (regardless of whether these data were observed or actively provided by the data subject, or a combination thereof).[84] Inferences about data subjects can be made both by the social media provider and the targeter.

80. For example, by virtue of monitoring the behaviour of its users over a long period of time, both on and off the social media (e.g. pages visited, time spent on each page, number of reconnections to that page, words searched, hyperlinks followed, "likes" given), the social media provider may be able to infer information regarding the interests and other characteristics of the user of the social media. In the same vein, a targeter might also be able to infer data about specific individuals and use that knowledge when targeting him or her to display ads on his or her social media page.

Example 7:

Mrs Delucca often "likes" photos posted by the Art Gallery "Beautifulart" by impressionist painter Pataolito on its social media page. Museum Z is looking to attract individuals who are interested in impressionist paintings in light of its upcoming exhibition. Museum Z uses the following targeting criteria offered by the social media provider: "interested in impressionism", gender, age and place of residence. Mrs Delucca subsequently receives targeted advertisement by Museum Z related to the upcoming exhibition of Museum Z on her social media page.

Example 8:

Mr Leon has indicated on his social media page that he is interested in sports. He has downloaded an application on his mobile phone to follow the latest results of his favorite sport games, has set on his browser the page www.livesportsresults.com as his homepage on his laptop, often uses his desktop computer at work to search for the latest sports results on the internet. He also visits a number of online gambling websites. The social media provider tracks Mr Leon' online activity across

[81] Article 29 Working Party, Opinion on profiling and automated decision making, WP 251, rev. 01, p. 15, see also Article 29 WP, Opinion on legitimate interest, p. 32 and 48: «Overall, there is an imbalance between the company's legitimate interest and the protection of users' fundamental rights and Article 7(f) should not be relied on as a legal ground for processing. Article 7(a) would be a more appropriate ground to be used, provided that the conditions for a valid consent are met».
[82] Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities, paragraph 41.
[83] European Data Protection Board, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0, 8 October 2019, paragraph 1.
[84] See also Article 29 Data Protection Working Party, Guidelines on the right to data portability, WP 242 rev.01, 5 April 2017, p. 10.

his multiple devices, i.e. his laptop, his cell mobile phone, and his desktop computer. Based on this activity and all the information provided by Mr Leon, the social media provider infers that he will be interested in online betting. In addition, the social media platform has developed targeting criteria enabling companies to target people who are likely to be impulsive and have a lower income. The online betting company "bestpaydayloans" wishes to target users that are interested in betting and that are likely to be betting heavily. It therefore selects the criteria offered by the social media provider to target the audience to whom its advertisement should be displayed.

5.4.1 Roles

81. For what concerns the determination of the roles of the different actors, the EDPB notes the following: in Example 7, joint controllership exists between Museum Z and the social media provider concerning the processing of personal data for the purposes of targeted advertising, taking into account the collection of these data via the 'like'-functionality on the social media platform, and the 'analysis' undertaken by the social media provider in order to offer the targeting criterion ("interested in impressionism") to the targeter fitting the purpose of finally displaying the advertisement.[85]

82. In Example 8, joint control exists between "bestpaydayloans" and the social media provider in relation to the processing operations jointly determined, in this case the selection of targeting criteria and subsequent display of the advertisement, as well as any reporting relating to the targeting campaign.

5.4.2 Legal basis

83. Targeting of social media users on the basis of inferred data for advertising purposes typically involves profiling.[86] The WP29 has previously clarified that according to the GDPR, profiling is an automated processing of personal data which aims at evaluating personal aspects, in particular to analyse or make predictions about individuals, adding that "*[t]he use of the word 'evaluating' suggests that profiling involves some form of assessment or judgement about a person*".[87] Profiling may be lawful by reference to any of the legal grounds in Article 6(1) GDPR, subject to the validity of this legal basis.

84. In Example 7, Article 5(3) of the ePrivacy Directive is applicable, insofar as the display of the advertisement on Mrs. Delucca's page related to the painter Pataolito requires a read/write operation to match this "like" with information previously held on her by the social media provider. Consent will therefore be required for these operations.

85. For what concerns Example 8, the EDPB recalls that in the case of automated decision-making which produces legal effects or similarly significantly affects the data subject, as set out in Article 22 GDPR data controllers may rely on the following exceptions:

- explicit consent of a data subject;
- the necessity of the automated decision-making for entering into, or performance of, a contract; or
- authorisation by Union or Member State law to which the controller is subject.

[85] As regards social media pages, joint controllership conditions may also be met in relation to statistical information provided by the social media provider to the page administrator: see CJEU C-210/16, *Wirtschaftsakademie*.
[86] The EDPB notes that profiling may have occurred in previous examples as well.
[87] Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP251rev.01, p. 7.

86. WP29 has already stated that "*In many typical cases the decision to present targeted advertising based on profiling will not have a similarly significant effect on individuals (…). However, it is possible that it may do, depending upon the particular characteristics of the case, including:*

- *the intrusiveness of the profiling process, including the tracking of individuals across different websites, devices and services;*
- *the expectations and wishes of the individuals concerned;*
- *the way the advert is delivered; or*
- *using knowledge of the vulnerabilities of the data subjects targeted.*"[88]

87. Where the profiling undertaken by the social media provider is likely to have a "similarly significant [effect]" on a data subject, Article 22 shall be applicable. An assessment as to whether targeting will "similarly significantly [effect]" a data subject will need to be conducted by the controller (or joint controllers, as the case may be) in each instance with reference to the specific facts of the targeting.

88. In such circumstances as described in Example 8, the display of online betting advertisements may fall under the scope of Article 22 GDPR (targeting financially vulnerable persons that are interested in online betting which have the potential to significantly and adversely affect his financial situation). Therefore, in accordance with Article 22, explicit consent would be required. Furthermore, the use of tracking techniques triggers the applicability of Article 5(3) of the ePrivacy Directive, resulting in a requirement of prior consent. Finally, the EDPB recalls that for the processing to be lawful, the controller must conduct a case-by-case assessment, and that obtaining consent does not reduce other obligations to observe the requirements of fairness, necessity, proportionality and data quality, as stated in Article 5 GDPR.

6 TRANSPARENCY AND RIGHT OF ACCESS

89. Article 5(1)(a) GDPR states that personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject. Article 5(1)(b) GDPR also states that personal data shall be collected for specified, explicit and legitimate purposes. Articles 12, 13 and 14 GDPR contain specific provisions on the transparency obligations of the data controller. Finally, recital 39 states that "*it should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed*".[89]

90. Information presented to data subjects in respect of the way in which their personal data are processed, should be, in all cases, concise, transparent, in an intelligible and easily accessible form, using clear and plain language.

91. The EDPB recalls that the mere use of the word "advertising" would not be enough to inform the users that their activity is being monitored for the purpose of targeted advertising. It should be made transparent to individuals what types of processing activities are carried out and what this means for the data subject in practice. Data subjects should be informed in an easily understandable language if a profile will be built based on their online behaviour on the platform or on the targeter's website, respectively, by the social platform and by the targeter, providing information to the users on the types of personal data collected to build such profiles and ultimately allow targeting and behavioural

[88] Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP251rev.01, p. 22.
[89] See also Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, WP260 rev.01, 11 April 2018, https://ec.europa.eu/newsroom/Article29/item-detail.cfm?item_id=622227

advertising by targeters.[90] Users should be provided with the relevant information directly on the screen, interactively and, where appropriate or necessary, through layered notices.[91]

6.1 Essence of the arrangement and information to provide (Article 26 (2) GDPR)

92. According to Article 26(1) GDPR, joint controllers "*shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects*".

93. A further expression of the transparency principle is the obligation to make the essence of the joint controllership arrangement available to the data subject according to Article 26 (2) GDPR. Indeed, Article 26 GDPR requires joint controllers to take appropriate measures to ensure that data subjects are made aware of the allocation of responsibilities.

94. As a matter of principle, the information provided to the data subject must cover all aspects of the data processing operation(s) for which the joint controllers are jointly responsible. Indeed, the data subject is entitled to receive all information (including regarding envisaged subsequent processing where there is joint controllership) at the outset, so that the information is fair and appropriate. More precisely, this joint arrangement needs to ensure that the data subject will be provided information required by Articles 13 and 14 GDPR, including on their shared or closely linked purposes, storage periods, transmission to third parties etc., which need to be communicated to the data subject upon collection of the data or before the processing starts. The arrangement needs to make it clear where the responsibilities lie in this regard. To meet these requirements, such arrangement must contain (or reference) clear and comprehensive information in respect of the processing to which it relates with explanations, where appropriate, on the various phases and actors of the processing.[92]

95. Although both joint controllers are subject to the duty to inform where there is joint responsibility, they can mutually agree that one of them shall be tasked with providing the initial information to data subjects, especially in cases where only one of the controllers interacts with the users prior to processing, for example on its website[93]. This exchange of information to provide to the data subject should be an integral part of the joint arrangement (e.g. an appendix). In case one of the joint controllers does not have all information in detail because, for example, it does not know the exact technical execution of the processing activities, the other joint controller shall provide all necessary information to enable him to provide the data subject with full information in accordance with Articles 13 and 14 GDPR.

96. The EDPB notes that controllers are not directly responsible for providing the information required by Articles 13 and 14 GDPR in relation to further processing operations that do not fall under the scope of joint controllership. Therefore, the targeter is not directly responsible for providing the information relating to any further processing which will be carried out by the social media platform.[94]

[90] Ref. to EDPB Guidelines on transparency under Regulation 2016/679.
[91] Article 29 Working Party, Guidelines on consent under Regulation 2016/679, WP259 rev. 01., para 24, 35.
[92] Opinion 1/2010 on the concepts of "controller" and "processor", WP 169, p. 28.
[93] CJEU *Fashion ID*, para 102, 105.
[94] As clarified in the EDPB Guidelines 7/2020 on concepts of the controller and processor in the GDPR, each controller's duty, to ensure that the data are not further processed in a manner that is incompatible with the

97. However, the EDPB emphasizes that the joint controller who intends to further use the personal data has specific obligations of information for this further processing where there is no joint responsibility, according to Article 14(4) of the GDPR, as well as obligations of compatibility of the further processing under Article 6(4).For example, the targeter and social media provider could agree that the targeter will provide certain information on behalf of the social media provider. The social media provider, however, remains ultimately responsible for ensuring that the data subject has been provided with the relevant information in relation to all the processing activities under its control.

> In Example 3 (Mr. Lopez being targeted for advertisement for Bank X on his social media page following the upload by the Bank of his email address to the social media provider), the Bank needs to inform Mr. Lopez that his email address will be used for advertising, via the social media provider, of offers linked to the bank services. Any further processing by the social media provider must be lawful and compatible with the purposes for which the Bank collected the data.
>
> In addition, to the extent that the social media provider intends to further process Mr. Lopez's email for another purpose, it must ensure that Mr. Lopez is provided with the information required by Article 14(4) GDPR prior to doing so.
>
> The social media provider and the Bank may agree that the Bank will provide Mr. Lopez with the relevant information on behalf of the social media provider. Even if that is the case, however, the social media provider remains ultimately responsible for ensuring that the data subject has been provided with the relevant information in relation to all the processing activities for which it is (alone) responsible. This obligation would not apply if Mr. Lopez has already been informed by the Bank of this processing, according to Article 14(5)(a) GDPR.
>
> These transparency obligations are to be considered without prejudice of the specific obligations applicable to legal basis considerations.

98. Each joint controller is responsible for ensuring that that the essence of the arrangement is made available to the data subject. In practice, the essence of the arrangement should be directly available on the platform, referred to in its privacy policy, and also made directly accessible by a link, for example, in the targeter's page on the social media platform or in links such as "why am I seeing this ad?".

6.2 Right of access (Article 15)

99. Data controllers must enable users to easily and fully exercise their data subjects' rights. An easy-to-use and efficient tool should be available for the data subject to ensure the easy exercise of all of their rights, at any time, in particular the right to erasure, to object, and the right of access pursuant to

purposes for which they were originally collected by the controller sharing the data. It should be good practice that the controller that intends to process personal data for further purposes provides sufficient means to the other controller that transmits personal data to ascertain that there is indeed a legal basis, which would likely be consent, and data subjects have been properly informed as this would enable the targeter to ensure that the transfer to the social media provider is lawful.

Article 15 GDPR.[95] The following paragraphs focus on how and by whom the right of access should be accommodated in the context of targeting of social media users.[96]

100. In general, to fulfill the requirements of Article 15 (1) GDPR and to ensure full transparency, controllers may want to consider implementing a mechanism for data subjects to check their profile, including details of the information and sources used to develop it. The data subject should be able to learn the identity of the targeter, and controllers should facilitate access to information regarding the targeting, including the targeting criteria that were used, as well as the other information required by Article 15 GDPR.[97]

101. As regards the kind of access to be provided to data subjects, recital 63 advises that *"[w]here possible, the controller should be able to provide remote access to a secure system which would provide the data subject with direct access to his or her personal data*." The specific features of social media providers - the online environment, the existence of a user account - suggest the possibility to easily grant the data subject with remote access to the personal data concerning him or her in accordance with Article 15 (1), (2) GDPR. Remote access in this case can be regarded as the most "appropriate measure" in the sense of Article 12(1) GDPR, also taking into account the fact that this is a typical situation "where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected" (see recital 58, which explicitly adds "online advertising" as concrete example). In addition, if requested, social media users who have been targeted should also be given a copy of the personal data relating to them in accordance with Article 15(3) GDPR.

102. According to Article 15(1)(c) GDPR, the user shall have access in particular to information on "*the recipients or categories of recipients to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations*". According to Article 4(9), the term "recipient" refers to a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether they are a third party or not. A targeter will not necessarily be a "recipient" of the personal data (see Example 1), as the personal data might not be disclosed to it, but it will receive statistics of the targeted customers in aggregated or anonymised form, e.g. as part of its campaign, or in a performance review of the same. Nevertheless, to the extent that the targeter acts as a joint controller, it must be identified as such to the social media user.

103. Although Article 15 GDPR is not explicitly identified in Article 26(1) GDPR, the wording of this Article refers to all "responsibilities for compliance" under GDPR, which includes Article 15 GDPR.

104. In order to enable data subjects to exercise their rights in an effective and easily accessible way, the arrangement between the social media provider and the targeter may designate a single point of contact for data subjects. Joint controllers are in principle free to determine amongst themselves who should be in charge of responding to and complying with data subject requests, but they cannot

[95] Article 15 (1), (2) GDPR detail the information to be given to the data subject asking for access to her data. Article 15 (3), (4) GDPR regulate the right to obtain a copy.
[96] See EDPB, Guidelines on transparency under Regulation 2016/679, p. 35.
[97] For further details regarding information pursuant to Art. 15 GPDR in the context of profiling, see Art. 29 Data Protection Working Party, WP 251rev.01, p. 17 for ("*Article 15 gives the data subject the right to obtain details of any personal data used for profiling, including the categories of data used to construct a profile. In addition to general information about the processing, pursuant to Article 15(3), the controller has a duty to make available the data used as input to create the profile as well as access to information on the profile and details of which segments the data subject has been placed into*"). It is important that such information should be tailored to the particular situation of the data subject, complementing any information already given under Articles 1 and 14.

exclude the possibility for the data subject to exercise his or her rights in respect of and against each of them (Article 26 (3) of the GDPR). Hence, targeters and social media providers must ensure that a suitable mechanism is in place to allow the data subjects to obtain access to his or her personal data in a user-friendly manner (including the targeting criteria used) and all information required by Article 15 of the GDPR.

7 DATA PROTECTION IMPACT ASSESSMENTS (DPIA)

105. In principle, prior to initiating the envisaged targeting operations, both joint controllers should check the list of processing operations "likely to result in a high risk" adopted at national level under Article 35(4) and recitals (71), (75) and (91) GDPR to determine if the designated targeting matches any of the types of processing operations subject to the requirement to conduct a DPIA. To assess whether the envisaged targeting operations are "likely to result in a high risk" and whether a DPIA is required, the criteria identified in the guidelines on DPIA should also be taken into account[98], as well as the lists that supervisory authorities have established of the kind of processing operations which are subject to the requirement for a data protection impact assessment (pursuant to Article 35(4)).

106. In some cases, the nature of the product or service advertised, the content of the message or the way the advert is delivered might produce effects on individuals whose impact has to be further assessed. This might be the case, for example, with products which are targeted at vulnerable people. Additional risks may emerge depending on the purposes of the advertising campaign and its intrusiveness, or if the targeting involves the processing of observed, inferred or derived personal data.

107. In addition to the obligations specifically referred to in Article 26 (1) GDPR, joint controllers should also consider other obligations when determining their respective obligations. As stated in the EDPB guidelines on DPIAs "When the processing operation involves joint controllers, they need to define their respective obligations precisely".

108. As a consequence, both joint controllers need to assess whether a DPIA is necessary. If a DPIA is necessary, they are both responsible for fulfilling this obligation. The EDPB recalls that the DPIA should tackle the entire processing of personal data, which means that in principle both joint controllers need to take part in the realization of the DPIA. In this context, both controllers need to ensure that they have a sufficient level of information on the processing to carry out the required DPIA.[99]This implies that "each data controller should express his needs and share useful information without either compromising secrets (e.g.: protection of trade secrets, intellectual property, confidential business information) or disclosing vulnerabilities".[100]

109. In practice, it is possible that joint controllers decide that one of them shall be tasked with carrying out the DPIA as such. This should then be specified in the joint arrangement, without prejudice to the existence of joint responsibility as such. It may indeed be that one of the controllers is better placed to assess certain processing operations. For example, this controller may, depending on the context,

[98] See EDPB Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, wp248rev.0.
[99] The EDPB reiterates that a DPIA is not required when the nature, scope, context and purposes of the processing are very similar to the processing for which DPIA have been carried out. In such cases, results of DPIA for similar processing can be used, see Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP 248 rev.01, p. 12.
[100] *Idem*, page 8.

be the one with a higher degree of control and knowledge of the targeting process in particular on the back-end of the deployed system, or on the means of the processing.

110. Every DPIA must include measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data, and to demonstrate compliance with the GDPR taking into account the rights and legitimate interests of data subjects and other persons concerned. If the identified risks cannot be sufficiently addressed (i.e. the residual risks remain high), the joint controllers are each responsible for ensuring a prior consultation with the relevant supervisory authorities. If the targeting would infringe the GDPR, in particular because the risks have insufficiently been identified or mitigated, the targeting should not take place.

> Example 9:
>
> The political party "Letschangetheworld" wishes to encourage social media users to vote for a particular political candidate in the upcoming elections. They wish to target elderly people living in rural areas of the country, who regularly go to church, and who have not travelled abroad in the past 2 years.

111. There is joint controllership between the social media platform and the political party, for the matching of the profile and the display of the targeted advertisement. The assessment of whether a DPIA is required needs to be carried out both by the Letschangetheworld political party and the social media platform. Indeed, in this example, they both have sufficient knowledge on the criteria that are being used to target the individuals in order to see that the processing is likely to result in a high risk.

112. If a DPIA is necessary, the joint arrangement should address the question of how the controllers should carry it and ensure that a relevant exchange of knowledge takes place. In this example, it may be that the social media platform is better placed to assess certain processing operations, insofar as the political party merely selects general targeting criteria.

8 SPECIAL CATEGORIES OF DATA

8.1 What constitutes a special category of data

113. The GDPR provides specific protection for personal data that are particularly sensitive in relation to individuals' fundamental rights and freedoms. Such data are defined in Article 9 GDPR as special categories of personal data and include data about an individual's health, racial or ethnic origin, biometry, religious or philosophical belief, political opinion, trade union membership, sex life or sexual orientation.

114. Controllers may only process special categories of data if they can meet one of the conditions set out in Article 9(2) GDPR, such as having obtained the data subject's explicit consent or the data have been manifestly made public by the data subject. In addition to the conditions in Article 9 GDPR, processing of special categories of data must rely on a legal basis laid down in Article 6 GDPR and be carried out in accordance with the fundamental principles set out in Article 5 GDPR.

115. Furthermore, the processing of special categories of personal data is relevant when assessing appropriate measures according to Articles 24, 25, 28 and 32 GDPR, but also to determine whether a DPIA must be carried out according to Article 35 GDPR, and whether a data protection officer must be appointed under Article 37 GDPR.

116. In the context of social media and targeting, it is necessary to determine whether the processing of personal data involves "special categories of data" and if such data are processed by the social media provider, the targeter or both. If special categories of personal data are processed, it must be determined whether and under what conditions the social media provider and the targeter can lawfully process such data.

117. If the social media provider processes the special category of data for targeting purposes, it must find a legal basis for the processing in Article 6 GDPR and rely on an exemption in Article 9(2) GDPR, such as explicit consent according to Article 9(2)(a) GDPR. If a targeter engages a social media provider and requests that the social media provider targets users based on this special category of data, the targeter will be jointly responsible with the social media provider for the processing of the special category data.

118. The following legal analysis will explore different situations when such processing may take place and their legal implications.

8.1.1 Explicit special categories of data

119. At times, personal data being processed clearly falls within the definition of special categories of data, e.g. in case of a direct statement about a person being member of a certain political party or religious association.

> Example 10:
>
> Ms. Flora states explicitly in her social media profile that she is a member of the GreenestPlanet political Party. The environmental organisation "Long live the Earth" wants to target social media users that are members of the GreenestPlanet political party in order to address targeted messages to them.

120. In Example 10, the social media provider and the environmental organisation are acting as joint controllers.[101] Insofar as the environmental organisation requests the social media provider to target users based on their political opinion, both controllers contribute to the processing of special categories of data as defined by Article 9 GDPR. Processing of these data are in principle prohibited according to Article 9(1). Both the social media provider and the environmental organisation must therefore be able to rely on one of the exemptions in Article 9(2) for their processing. In addition to that, they must also both have a legal basis according to Article 6. Out of the exemptions in Article 9(2), it appears that the only applicable exemptions in this situation would be to obtain the data subject's explicit consent, under Article 9(2)(a) GDPR, or the exemption that Ms. Flora manifestly made the personal data public, under Article 9 (2)(e) GDPR.

8.1.2 Inferred and combined special categories of data

121. Assumptions or inferences regarding special category data, for instance that a person is likely to vote for a certain party after visiting a page preaching liberal opinions, would also constitute a special category of personal data. Likewise, as previously stated by the EDPB, *"profiling can create special category of data by inference from data which is not special category of data in its own right, but becomes so when combined with other data. For example, it may be possible to infer someone's state of health from the records of their food shopping combined with data on the quality and energy content of foods"*. [102]

[101] See the analysis in chapter 5.2.1.

[102] Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP251rev.01, page 15.

122. For instance, the processing of a mere statement, or a single piece of location data or similar, which reveals that a user has (either once or on a few occasions) visited a place typically visited by people with certain religious beliefs will generally not in and of itself be considered as processing of special categories of data. However, it may be considered as processing of special categories of data if these data are combined with other data or because of the context in which the data are processed or the purposes for which they are being used.

> Example 11:
>
> The profile on Mr. Novak's social media account only reveals general information such as his name and domicile, but a status update reveals that he has visited the City Church frequently where he attended a religious service. Later on, the City Church wants to target its visitors with religious messages in order to encourage Christian people to join the congregation. In such circumstances, the use of personal data in Mr. Novak's status update for such a targeting purposes amounts to the processing of special categories of personal data.

123. If a social media provider or a targeter uses observed data to categorise users as having certain religious, philosophical or political beliefs - regardless of whether the categorization is correct/true or not - this categorisation of the user must obviously be seen as processing of special category of personal data in this context. As long as the categorisation enables targeting based on special category data, it does not matter how the category is labelled.

> Example 12:
>
> Mr. Sifuentes provides information in his social media profile in the shape of regular status updates, check-ins, etc., which indicate that he regularly takes part in activities arranged by the "Mind, Body and Spirit Movement". Even though no explicit statement on philosophical belief is provided, all updates, likes, check-ins and similar data provided by the user when collated, strongly indicate that Mr. Sifuentes has a certain philosophical belief.

> Example 13:
>
> A social media provider uses information actively provided by Ms. Allgrove on her social media profile page about her age, interests and address and combines it with observed data about the websites visited by her and her "likes" on the social media platform. The social media provider uses the data to infer that Ms. Allgrove is a supporter of left-wing liberal politics and places her in the "interested in left wing liberal politics" targeting category, and makes this category available to targeters for targeted advertising.

124. In Example 12, the vast information and the absence of measures to prevent targeting based on special category data implies that a processing of special categories of data is taking place. However, the mere fact that a social media provider processes large amounts of data which potentially could be used to infer special categories of data does not automatically mean that the processing falls under Article 9 GDPR. Article 9 will not be triggered if the social media provider's processing does not result in inference of special categories of data and the social media provider has taken measures to prevent that such data can be inferred or used for targeting. In any case, processing of a large amount of personal data about users may entail specific risks for the rights and freedoms of natural persons, which have to be addressed by implementing appropriate security measures, as prescribed under Article 32 GDPR, and also by taking into account the outcome of the DPIA to be performed pursuant to Article 35 GDPR.

125. In Example 13, the offering as well as use of the targeting category "interested in left wing liberal politics" amounts to processing of special categories of data, as this category could easily be used as a proxy to target individuals who have left wing liberal political beliefs. By assigning an inferred political opinion to a user, the social media provider processes special categories of data. For the purpose of Article 9 GDPR, it is not relevant whether the user in fact is a supporter of left-wing liberal politics. Nor is it relevant that the targeting category is named "interested in..." and not "supporter of...", since the user is placed in the targeting category based on inferred political interests.

> Example 14:
>
> Mr. Svenson takes a career aptitude test developed, containing a psychological evaluation, by the company "YourPerfectJob" which is made available on a social media platform and makes use of the Application Programming Interface (API) provided by the social media provider. YourPerfectJob collects data about Mr. Svenson's education, employment status, age, hobbies, posts, email-address and connections. YourPerfectJob obtains the data through the API in accordance with the "permissions" granted by Mr. Svenson through his social media account. The stated purpose of the application is to predict what would be the best career path for a specific user.
>
> Without the knowledge or approval of the social media provider, YourPerfectJob uses this information to infer a number of personal aspects, including his personality traits, psychological profile and political beliefs. YourPerfectJob later decides to use this information to target Mr. Svenson on behalf of a political party, using of the email-based targeting feature of the social media provider, without adding any other targeting criteria offered by the social media provider.

In Example 14, the targeter processes special categories of personal data, whereas the social media provider does not. Indeed, the assessment and identification of Mr. Svenson's political belief occurs without the involvement of the social media provider.[103] In addition to triggering the general prohibition of Article 9 GDPR, the targeting mentioned in Example 14 also constitutes an infringement of the requirements concerning fairness, transparency and purpose limitation. Indeed, Mr. Svenson is not properly informed of the fact that the personal relating to him will be processed for political targeting, which in addition, does not seem compatible with a career aptitude test.

126. While processing activities of the social media provider in Example 14 do not amount to processing of special categories of data within the meaning of Article 9 GDPR, the social media provider is responsible for integrating the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of data subjects in accordance with Article 24 and 25 GDPR.

8.2 The Article 9(2) exception of special categories of data made manifestly public

[103] In Example 14, there is no joint controllership between the social media provider and YourPerfectJob at the moment of collection of personal data, because they do not jointly determine the purposes of the collection and subsequent or further processing of personal data for the purposes of Yourperfectjob at this stage of the processing. The EDPB would like to recall that the analysis on the roles and responsibilities needs to be done on a case by case basis, and that the conclusion on this specific example is without prejudice of any further work that can be carried out by the EDPB on APIs. The situation would of course be different if the social media provider, in addition to making the personal data available, also participated in the determination of purpose pursued by YourPerfectJob. In any event, joint controllership still exists between the targeter and the social media provider as regards the use of list-based targeting.

127. Article 9(2)(e) of the GDPR allows processing of special category of data in cases where the data have been manifestly made public by the data subject. The word "manifestly" implies that there must be a high threshold for relying on this exemption. The EDPB notes that the presence of a single element may not always be sufficient to establish that the data have been "manifestly" made public by the data subject. In practice, a combination of the following or other elements may need to be considered for controllers to demonstrate that the data subject has clearly manifested the intention to make the data public, and a case-by-case assessment is needed. The following elements may be relevant to help inform this assessment:

(i) the default settings of the social media platform (i.e. whether the data subject took a specific action to change these default private settings into public ones); or

(ii) the nature of the social media platform (i.e. whether this platform is intrinsically linked with the idea of connecting with close acquaintances of the data subject or creating intimate relations (such as online dating platforms), or if it is meant to provide a wider scope of interpersonal relations, such as professional relations, or microblogging, media sharing, social platforms to share online reviews, etc. ; or

(iii) the accessibility of the page where the sensitive data is published (i.e. whether the information is publicly accessible or if, for instance, the creation of an account is necessary before accessing the information); or

(iv) the visibility of the information where the data subject is informed of the public nature of the information that they publish (i.e. whether there is for example a continuous banner on the page, or whether the button for publishing informs the data subject that the information will be made public…); or

(v) if the data subject has published the sensitive data himself/herself, or whether instead the data has been published by a third party (e.g. a photo published by a friend which reveals sensitive data) or inferred.

128. The EDPB notes that the presence of a single element may not always be sufficient to establish that the data have been "manifestly" made public by the data subject. In practice, a combination of these or other elements may need to be considered for controllers to demonstrate that the data subject has clearly manifested the intention to make the data public.

> Example 15:
>
> Mr Jansen has opened an account on a microblogging social media platform. While completing his profile, he indicated that he is homosexual. Being a conservative, he chose to join conservative groups, knowing that he has been informed while subscribing that the messages he exchanges on the platform are public. A conservative political party wishes to target people who share the same political affiliations and sexual orientation as Mr. Jansen using the social media targeting tools.

129. Because members' sexual orientation is by default "private" and that Mr. Jansen has not taken any step to make it public, it cannot be considered as having been manifestly made public. In addition, the data relating to his political affiliation has not been made manifestly public, despite of (i) the nature of the microblogging social media platform, which is meant to share information with the wide public, and (ii) the fact that he has been informed of the public nature of the messages he publishes on the forums. In addition, although he has joined public forums relating to conservatism, he cannot be targeted on the basis of this sensitive data, because it is the social media platform that makes a deduction on Mr Janssen's political affiliation, and it was not the specific intention of the data subject to make this data manifestly public, all the more that this deduction may turn out to be false. He cannot

therefore be targeted on the basis of political affiliation data. In other words, the circumstances in each specific case have to be taken into account when assessing whether the data have manifestly been made public by the data subject.[104]

9 JOINT CONTROLLERSHIP AND RESPONSIBILITY

9.1 Joint controller arrangement and determination of responsibilities (Art. 26 GDPR)

130. Article 26 (1) GDPR requires joint controllers to determine – in a transparent manner – their respective responsibilities for compliance with the obligations of the GDPR in an arrangement, including, as explained above, the requirements for transparency.

131. In terms of scope, the EDPB considers that the arrangement between targeters and social media providers should encompass all processing operations for which they are jointly responsible (i.e. which are under their joint control). By concluding an arrangement that is only superficial and incomplete, targeters and social media providers would be in breach of non-compliance with their obligations under Article 26 of the GDPR.

> For instance, in Example 4 the arrangement should cover the entire processing of personal data where there is joint controllership, i.e. from the collection of personal data in the context of the visit by Mr. Schmidt of the website "BestBags.com" with a tracking pixel, to the display of the advertisement on his social media page, as well as any eventual reporting relating to the targeting campaign.

132. In order to develop a comprehensive arrangement, both the social media provider and the targeter must be aware of and have sufficiently detailed information regarding the specific data processing operations taking place. The arrangement between the targeter and the social media provider should therefore contain (or refer to) all necessary information to enable both parties to comply with their obligations under the GDPR, including their duty to comply with the principles under Article 5(1) GDPR and their duty to demonstrate their compliance according to Article 5(2) GDPR.

133. If, for example, the controller is considering to rely on Article 6(1)(f) GDPR as a legal basis, it is necessary, among other things, to know the extent of the data processing in order to be able to assess whether the interest of the controller(s) are overridden by the interests or fundamental rights and freedoms of the data subjects. Without sufficient information concerning the processing, such an assessment cannot be performed. The importance of including or referencing the necessary information in the context of a joint arrangement cannot be overstated, especially in situations where one of the parties almost exclusive has the knowledge and access to the information necessary for both parties to comply with the GDPR.

> For instance, in Example 1, when Company X is assessing whether it can rely on the legitimate interest as a legal basis to target men between the age of 30 and 45 and who have indicated that they are single, it is necessary that it has access to sufficient information concerning the processing carried out by the social media platform, including for instance for what concerns the additional

[104] The WP29 clarified in its Opinion on some key issues of the Law Enforcement Directive (WP 258, 29/11/2017, p. 10) that the expression "manifestly made public by the data subject" has to be interpreted to imply that the data subject was aware that the respective data will be publicly available which means to everyone, including authorities; therefore, "In case of doubt, a narrow interpretation should be applied…".

measures (such as the right to prior objection) put into place by the latter, to ensure that legitimate interests are not overridden by the data subject's interests or fundamental rights and freedoms.

134. In order to ensure that the rights of the data subject can be accommodated effectively, the EDPB takes the view that the purpose of the processing and the corresponding legal basis should be also reflected in the joint arrangement between targeters and social media providers who are joint controllers. Although the GDPR does not preclude joint controllers to use different legal basis for different processing operations they carry out, it is recommended to use, whenever possible, the same legal basis for a particular targeting tool and for a particular purpose. Indeed, if each stage of the processing is processed on a different legal basis, this would render the exercise of rights impracticable for the data subject (e.g. for one stage there would be a right to data portability, for another there would be a right to object).

135. As controllers the targeter and the social media provider are both responsible for ensuring that the principle of purpose limitation is complied with and should therefore incorporate appropriate provisions to that end within the joint arrangement.

For example, if the targeter wishes to use personal data provided to it by the data subject in order to target on social media, it must take appropriate measures to ensure that the data provided shall not be further used by the social media provider in a manner that is incompatible with those purposes, unless the valid consent of the data subject has been obtained pursuant to Article 6(4) of the GDPR.

In Example 3, the Bank X should ensure that there are appropriate provisions in the joint arrangement with the social media platform that Mr. Lopez' email address is not used for other purposes that advertising of offers linked to the bank services that he is already using without Mr. Lopez' consent.

Likewise, the social media provider must ensure that use of data for targeting purposes by the targeters is in compliance with the principles of purpose limitation, transparency and lawfulness.

136. Other obligations that should be considered by the targeter and social media provider in the context of their joint arrangement include: other general data protection principles contained in Article 5 GDPR, security of processing, data protection by design and by default, notifications and communications of personal data breaches, data protection impact assessments, the use of processors and transfers to third countries.

For instance, in Example 13, the joint arrangement should address the question of which of the controllers should carry a DPIA and ensure that a relevant exchange of knowledge takes place. In other words, the political party "Letschangetheworld" should ensure that it has a sufficient level of information, for instance on the security measures put into place by the social media platform, when a DPIA is carried out.

137. Finally, the joint arrangement between the social media provider and the targeter must contain specific information about how the obligations under the GDPR shall be fulfilled in practice. If there is no clarity as to the manner in which the obligations are to be fulfilled, in particular in relation to data subject rights, both the targeter and the social media provider will be considered as acting in violation of Article 26(1) GDPR. Moreover, in such cases, both (joint) controllers will not have implemented

appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the GDPR and therefore will have breached their obligations under Articles 5(2) and 24.

9.2 Levels of responsibility

138. The EDPB observes that targeters who wish to use targeting tools provided by a social media provider may be confronted with the need to adhere to pre-defined arrangements, without any possibility to negotiate or make modifications ('take it or leave it' conditions). The EDPB considers that such a situation does not negate the joint responsibility of the social media provider and the targeter and cannot serve to exempt either party from its obligations under the GDPR. Both parties to the joint arrangement are also bound to ensure that the allocation of responsibilities duly reflects their respective roles and relationships vis-à-vis data the subjects in a practical, truthful and transparent manner.

139. It is important to stress that an arrangement pursuant to Article 26 GDPR cannot override the legal obligations incumbent upon a (joint) controller. While joint controllers shall, in accordance with Article 26 GDPR "*determine their respective responsibilities for compliance*" with the GDPR, each controller remains, as a matter of principle, responsible for the compliance of processing. This means that each controller is – *inter alia* – responsible for compliance with the principles set out under Article 5(1) GDPR, including the principle of lawfulness established under Article 5(1)(a) GDPR.

140. However, the degree of responsibility of the targeter and of the social media provider in relation to specific obligations may vary. In *Wirtschaftsakademie*, the CJEU noted that "*the existence of joint responsibility does not necessarily imply equal responsibility of the various operators involved in the processing of personal data. [...] those operators may be involved at different stages of that processing of personal data and to different degrees, so that the level of responsibility of each of them must be assessed with regard to all the relevant circumstances of the particular case*". [105]

141. In other words, although joint controllers are both responsible for complying with the obligations under the GDPR, and although the data subject may exercise his or her rights as against each of the controllers, their level of responsibility must be assessed on their actual role in the processing. In *Google Spain*, the CJEU clarified that a controller must ensure, "*within the framework of its responsibilities, powers and capabilities*", that the processing of personal data meets the requirements of EU data protection law.[106]

142. When it comes to assessing the level of responsibility of targeters and social media providers, several factors may be relevant, such as the ability to influence the processing on a practical level, as well as the actual or constructive knowledge of each of the joint controllers. It is also important to be clear at what stage of the processing and to what extent or degree the targeter and the social media provider are responsible for the processing.[107]

In Example 1, Company X sets up an advertising campaign so that users corresponding to specific targeting criteria may be shown advertisements for the company on the social media platform. However, although it sets the parameters for the advertising campaign, it does not collect or have

[105] CJEU judgment of 05 June 2018, Wirtschaftsakademie, C-210/16, paragraph 43.
[106] See also CJEU, C-131/12, Google Spain ("responsibilities, powers and capabilities").
[107] The EDPB considers that in a variety of cases an assessment based on the criteria mentioned above (e.g. the data used to establish the targeting criteria, the matching of the data subject, the collection of consent) will likely lead to the outcome that it is the social media provider that has more factual influence on the processing and therefore has a higher degree of responsibility, depending on the specific targeting mechanism being used.

access to any personal data, nor does it have any direct contact with the data subject. Each of these elements may be relevant when assessing the level (or "degree") or responsibility of the targeter and social media provider in case a violation of the GDPR is established (e.g. in case of lack of transparency towards the data subject or failure to ensure lawfulness of processing). As indicated earlier, notwithstanding, both parties are obliged to undertake appropriate measures in order to meet the requirements of the GDPR and protect the rights of data subjects against unlawful forms of processing.

In Example 3, which involved list-based targeting, the situation is slightly different than Example 1. In Example 3, the bank initially collected the personal data and shared it with the social media provider for targeting purposes. In that case, the targeter has voluntarily caused the collection and transmission stage of the data processing. Each of these elements should be taken into account when assessing the level of responsibility of each actor and should be duly reflected in the terms of the joint arrangement.

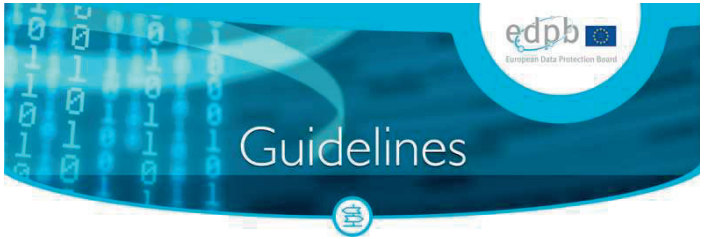
Similarly, in Example 4, in case of pixel-based targeting, it should be taken into account that the website operator enables the transmission of personal data to the social media provider. It is indeed the website "BestBags.com" that integrates a tracking pixel on its website so that it can target Mr Schmidt, although he has decided not to make a purchase[108]. The website is therefore actively involved in the collection and transmission of the data. As a joint controller, however, the social media provider is also under an obligation to undertake appropriate measures to meet the requirements of the GDPR and protect the rights of data subjects against unlawful forms of processing. In this case, if the data subject's consent is sought, the joint controllers should agree upon the way in which consent is collected in practice.

143. When it comes to assessing the level of responsibility of social media provider, the EDPB observes that several targeting mechanisms rely on profiling and/or other processing activities previously undertaken by the social media provider. It is the social media provider who decides to process personal data of its users in such a manner to develop the targeting criteria which it makes available to targeters. In order to do so, the social media provider has independently made certain decisions regarding the processing, such as which categories of data shall be processed, which targeting criteria shall be offered and who shall have access (to what types of) personal data that is processed in the context of a particular targeting campaign. Such processing activities must also comply with the GDPR, prior to the offering of any targeting services.

144. The examples mentioned in the preceding paragraphs indicate the importance of clearly allocating responsibilities in the joint controller arrangement between social media providers and targeters. Even though the terms of the arrangement should in any case mirror the level of responsibility of each actor, a comprehensive arrangement which duly reflects the role and capabilities of each party is necessary not only to comply with Article 26 of the GDPR, but also for complying with other rules and principles of the GDPR.

145. Finally, the EDPB notes that insofar as the terms of the joint arrangement between the social media provider and the targeter do not bind supervisory authorities, supervisory authorities may exercise their competences and powers in relation to either joint controller, as long as the joint controller in question is subject to the competence of that supervisory authority.

[108] In addition, as BestBags.com has integrated the social media tracking pixel on its website, it is also responsible for complying with the ePrivacy Directive requirements regarding this tool, which, given that the pixel also facilitates the processing of personal data, is also of importance when determining the level of responsibility.



Guidelines 07/2020 on the concepts of controller and processor in the GDPR

Version 2.0

Adopted on 07 July 2021

Version history

Version 2.0	7 July 2021	Adoption of the Guidelines after public consultation
Version 1.0	2 September 2020	Adoption of the Guidelines for public consultation

EXECUTIVE SUMMARY

The concepts of controller, joint controller and processor play a crucial role in the application of the General Data Protection Regulation 2016/679 (GDPR), since they determine who shall be responsible for compliance with different data protection rules, and how data subjects can exercise their rights in practice. The precise meaning of these concepts and the criteria for their correct interpretation must be sufficiently clear and consistent throughout the European Economic Area (EEA).

The concepts of controller, joint controller and processor are *functional* concepts in that they aim to allocate responsibilities according to the actual roles of the parties and *autonomous* concepts in the sense that they should be interpreted mainly according to EU data protection law.

Controller

In principle, there is no limitation as to the type of entity that may assume the role of a controller but in practice it is usually the organisation as such, and not an individual within the organisation (such as the CEO, an employee or a member of the board), that acts as a controller.

A controller is a body that *decides* certain key elements of the processing. Controllership may be defined by law or may stem from an analysis of the factual elements or circumstances of the case. Certain processing activities can be seen as naturally attached to the role of an entity (an employer to employees, a publisher to subscribers or an association to its members). In many cases, the terms of a contract can help identify the controller, although they are not decisive in all circumstances.

A controller determines the purposes and means of the processing, i.e. the *why* and *how* of the processing. The controller must decide on both purposes and means. However, some more practical aspects of implementation ("non-essential means") can be left to the processor. It is not necessary that the controller actually has access to the data that is being processed to be qualified as a controller.

Joint controllers

The qualification as joint controllers may arise where more than one actor is involved in the processing. The GDPR introduces specific rules for joint controllers and sets a framework to govern their relationship. The overarching criterion for joint controllership to exist is the joint participation of two or more entities in the determination of the purposes and means of a processing operation. Joint participation can take the form of a *common decision* taken by two or more entities or result from *converging decisions* by two or more entities, where the decisions complement each other and are necessary for the processing to take place in such a manner that they have a tangible impact on the determination of the purposes and means of the processing. An important criterion is that the processing would not be possible without both parties' participation in the sense that the processing by each party is inseparable, i.e. inextricably linked. The joint participation needs to include the determination of purposes on the one hand and the determination of means on the other hand.

Processor

A processor is a natural or legal person, public authority, agency or another body, which processes personal data on behalf of the controller. Two basic conditions for qualifying as processor exist: that it is a separate entity in relation to the controller and that it processes personal data on the controller's behalf.

The processor must not process the data otherwise than according to the controller's instructions. The controller's instructions may still leave a certain degree of discretion about how to best serve the controller's interests, allowing the processor to choose the most suitable technical and organisational means. A processor infringes the GDPR, however, if it goes beyond the controller's instructions and starts to determine its own purposes and means of the processing. The processor will then be considered a controller in respect of that processing and may be subject to sanctions for going beyond the controller's instructions.

Relationship between controller and processor

A controller must only use processors providing sufficient guarantees to implement appropriate technical and organisational measures so that the processing meets the requirements of the GDPR. Elements to be taken into account could be the processor's expert knowledge (e.g. technical expertise with regard to security measures and data breaches); the processor's reliability; the processor's resources and the processor's adherence to an approved code of conduct or certification mechanism.

Any processing of personal data by a processor must be governed by a contract or other legal act which shall be in writing, including in electronic form, and be binding. The controller and the processor may choose to negotiate their own contract including all the compulsory elements or to rely, in whole or in part, on standard contractual clauses.

The GDPR lists the elements that have to be set out in the processing agreement. The processing agreement should not, however, merely restate the provisions of the GDPR; rather, it should include more specific, concrete information as to how the requirements will be met and which level of security is required for the personal data processing that is the object of the processing agreement.

Relationship among joint controllers

Joint controllers shall in a transparent manner determine and agree on their respective responsibilities for compliance with the obligations under the GDPR. The determination of their respective responsibilities must in particular regard the exercise of data subjects' rights and the duties to provide information. In addition to this, the distribution of responsibilities should cover other controller obligations such as regarding the general data protection principles, legal basis, security measures, data breach notification obligation, data protection impact assessments, the use of processors, third country transfers and contacts with data subjects and supervisory authorities.

Each joint controller has the duty to ensure that they have a legal basis for the processing and that the data are not further processed in a manner that is incompatible with the purposes for which they were originally collected by the controller sharing the data.

The legal form of the arrangement among joint controllers is not specified by the GDPR. For the sake of legal certainty, and in order to provide for transparency and accountability, the EDPB recommends that such arrangement be made in the form of a binding document such as a contract or other legal binding act under EU or Member State law to which the controllers are subject.

The arrangement shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects and the essence of the arrangement shall be made available to the data subject.

Irrespective of the terms of the arrangement, data subjects may exercise their rights in respect of and against each of the joint controllers. Supervisory authorities are not bound by the terms of the arrangement whether on the issue of the qualification of the parties as joint controllers or the designated contact point.

TABLE OF CONTENTS

EXECUTIVE SUMMARY 3
INTRODUCTION 7
PART I – CONCEPTS 8
1 GENERAL OBSERVATIONS 8
2 DEFINITION OF CONTROLLER 9
2.1 Definition of controller 9
2.1.1 "Natural or legal person, public authority, agency or other body" 10
2.1.2 "Determines" 11
2.1.3 "Alone or jointly with others" 14
2.1.4 "Purposes and means" 14
2.1.5 "Of the processing of personal data" 17
3 DEFINITION OF JOINT CONTROLLERS 18
3.1 Definition of joint controllers 18
3.2 Existence of joint controllership 18
3.2.1 General considerations 18
3.2.2 Assessment of joint participation 19
3.2.3 Situations where there is no joint controllership 24
4 DEFINITION OF PROCESSOR 25
5 DEFINITION OF THIRD PARTY/RECIPIENT 28
PART II – CONSEQUENCES OF ATTRIBUTING DIFFERENT ROLES 30
1 RELATIONSHIP BETWEEN CONTROLLER AND PROCESSOR 30
1.1 Choice of the processor 30
1.2 Form of the contract or other legal act 31
1.3 Content of the contract or other legal act 34
1.3.1 The processor must only process data on documented instructions from the controller (Art. 28(3)(a) GDPR) 35
1.3.2 The processor must ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality (Art. 28(3)(b) GDPR) 36
1.3.3 The processor must take all the measures required pursuant to Article 32 (Art. 28(3)(c) GDPR) 37
1.3.4 The processor must respect the conditions referred to in Article 28(2) and 28(4) for engaging another processor (Art. 28(3)(d) GDPR). 37

1.3.5 The processor must assist the controller for the fulfilment of its obligation to respond to requests for exercising the data subject's rights (Article 28(3) (e) GDPR). 38
1.3.6 The processor must assist the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 (Art. 28(3)(f) GDPR). 38
1.3.7 On termination of the processing activities, the processor must, at the choice of the controller, delete or return all the personal data to the controller and delete existing copies (Art. 28(3)(g) GDPR). 40
1.3.8 The processor must make available to the controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller (Art. 28(3)(h) GDPR) 40
1.4 Instructions infringing data protection law 41
1.5 Processor determining purposes and means of processing 42
1.6 Sub-processors 42
2 CONSEQUENCES OF JOINT CONTROLLERSHIP 43
2.1 Determining in a transparent manner the respective responsibilities of joint controllers for compliance with the obligations under the GDPR 43
2.2 Allocation of responsibilities needs to be done by way of an arrangement 46
2.2.1 Form of the arrangement 46
2.2.2 Obligations towards data subjects 46
2.3 Obligations towards data protection authorities. 48

The European Data Protection Board

Having regard to Article 70 (1e) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, (hereinafter "GDPR" or "the Regulation"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018[1],

Having regard to Article 12 and Article 22 of its Rules of Procedure,

Whereas the preparatory work of these guidelines involved the collection of inputs from stakeholders, both in writing and at a stakeholder event, in order to identify the most pressing challenges;

HAS ADOPTED THE FOLLOWING GUIDELINES

INTRODUCTION

1. This document seeks to provide guidance on the concepts of controller and processor based on the GDPR's rules on definitions in Article 4 and the provisions on obligations in chapter IV. The main aim is to clarify the meaning of the concepts and to clarify the different roles and the distribution of responsibilities between these actors.

2. The concept of controller and its interaction with the concept of processor play a crucial role in the application of the GDPR, since they determine who shall be responsible for compliance with different data protection rules, and how data subjects can exercise their rights in practice. The GDPR explicitly introduces the accountability principle, i.e. the controller shall be responsible for, and be able to demonstrate compliance with, the principles relating to processing of personal data in Article 5. Moreover, the GDPR also introduces more specific rules on the use of processor(s) and some of the provisions on personal data processing are addressed - not only to controllers - but also to processors.

3. It is therefore of paramount importance that the precise meaning of these concepts and the criteria for their correct use are sufficiently clear and shared throughout the European Union and the EEA.

4. The Article 29 Working Party issued guidance on the concepts of controller/processor in its opinion 1/2010 (WP169)[2] in order to provide clarifications and concrete examples with respect to these concepts. Since the entry into force of the GDPR, many questions have been raised regarding to what extent the GDPR brought changes to the concepts of controller and processor and their respective roles. Questions were raised in particular to the substance and implications of the concept of joint controllership (e.g. as laid down in Article 26 GDPR) and to the specific obligations for processors laid down in Chapter IV (e.g. as laid down in Article 28 GDPR). Therefore, and as the EDPB recognizes that the concrete application of the concepts needs further clarification, the EDPB now deems it necessary to give more developed and specific guidance in order to ensure a consistent and harmonised approach throughout the EU and the EEA. The present guidelines replace the previous opinion of Working Party 29 on these concepts (WP169).

5. In part I, these guidelines discuss the definitions of the different concepts of controller, joint controllers, processor and third party/recipient. In part II, further guidance is provided on the consequences that are attached to the different roles of controller, joint controllers and processor.

[1] References to "Member States" made throughout this document should be understood as references to "EEA Member States".
[2] Article 29 Working Party Opinion 1/2010 on the concepts of "controller" and "processor" adopted on 16 February 2010, 264/10/EN, WP 169.

PART I – CONCEPTS

1 GENERAL OBSERVATIONS

6. The GDPR, in Article 5(2), explicitly introduces the accountability principle which means that:

   – the controller shall be *responsible for the compliance* with the principles set out in Article 5(1) GDPR; and that
   – the controller shall be able to *demonstrate compliance* with the principles set out in Article 5(1) GDPR.

   This principle has been described in an opinion by the Article 29 WP [3] and will not be discussed in detail here.

7. The aim of incorporating the accountability principle into the GDPR and making it a central principle was to emphasize that data controllers must implement appropriate and effective measures and be able to demonstrate compliance. [4]

8. The accountability principle has been further elaborated in Article 24, which states that the controller shall implement appropriate technical and organisational measures to ensure and to be able **to demonstrate** that processing is performed in accordance with the GDPR. Such measures shall be reviewed and updated if necessary. The accountability principle is also reflected in Article 28, which lays down the controller's obligations when engaging a processor.

9. The accountability principle is directly addressed to the controller. However, some of the more specific rules are addressed to both controllers and processors, such as the rules on supervisory authorities' powers in Article 58. Both controllers and processors can be fined in case of non-compliance with the obligations of the GDPR that are relevant to them and both are directly accountable towards supervisory authorities by virtue of the obligations to maintain and provide appropriate documentation upon request, co-operate in case of an investigation and abide by administrative orders. At the same time, it should be recalled that processors must always comply with, and act only on, instructions from the controller.

10. The accountability principle, together with the other, more specific rules on how to comply with the GDPR and the distribution of responsibility, therefore makes it necessary to define the different roles of several actors involved in a personal data processing activity.

[3] Article 29 Working Party Opinion 3/2010 on the principle of accountability adopted on 13 July 2010, 00062/10/EN WP 173.
[4] Recital 74 GDPR.

11. A general observation regarding the concepts of controller and processor in the GDPR is that they have not changed compared to the Directive 95/46/EC and that overall, the criteria for how to attribute the different roles remain the same.

12. The concepts of controller and processor are *functional* concepts: they aim to allocate responsibilities according to the actual roles of the parties.[5]This implies that the legal status of an actor as either a "controller" or a "processor" must in principle be determined by its actual activities in a specific situation, rather than upon the formal designation of an actor as being either a "controller" or "processor" (e.g. in a contract).[6] This means that the allocation of the roles usually should stem from an analysis of the factual elements or circumstances of the case and as such is not negotiable.

13. The concepts of controller and processor are also *autonomous* concepts in the sense that, although external legal sources can help identifying who is a controller, it should be interpreted mainly according to EU data protection law. The concept of controller should not be prejudiced by other - sometimes colliding or overlapping - concepts in other fields of law, such as the creator or the right holder in intellectual property rights or competition law.

14. As the underlying objective of attributing the role of controller is to ensure accountability and the effective and comprehensive protection of the personal data, the concept of 'controller' should be interpreted in a sufficiently broad way, favouring as much as possible effective and complete protection of data subjects[7] so as to ensure full effect of EU data protection law, to avoid lacunae and to prevent possible circumvention of the rules, while at the same time not diminishing the role of the processor.

2 DEFINITION OF CONTROLLER

2.1 Definition of controller

15. A controller is defined by Article 4(7) GDPR as

> "***the natural or legal person, public authority, agency or other body*** *which,* ***alone or jointly with others, determines*** *the* ***purposes and means*** *of the* ***processing of personal data****; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be* ***provided for by Union or Member State law****".*

16. The definition of controller contains five main building blocks, which will be analysed separately for the purposes of these Guidelines. They are the following:

- "the natural or legal person, public authority, agency or other body"
- "determines"
- "alone or jointly with others"
- "the purposes and means"
- "of the processing of personal data".

2.1.1 "Natural or legal person, public authority, agency or other body"

17. The first building block relates to the type of entity that can be a controller. Under the GDPR, a controller can be "*a natural or legal person, public authority, agency or other body*". This means that, in principle, there is no limitation as to the type of entity that may assume the role of a controller. It might be an organisation, but it might also be an individual or a group of individuals.[8] In practice, however, it is usually the organisation as such, and not an individual within the organisation (such as the CEO, an employee or a member of the board), that acts as a controller within the meaning of the GDPR. As far as data processing within a company group is concerned, special attention must be paid to the question of whether an establishment may be acting as a controller or processor, e.g. when processing data on behalf of the parent company.

18. Sometimes, companies and public bodies appoint a specific person responsible for the implementation of the processing activity. Even if a specific natural person is appointed to ensure compliance with data protection rules, this person will not be the controller but will act on behalf of the legal entity (company or public body) which will be ultimately responsible in case of infringement of the rules in its capacity as controller. In the same vein, even if a particular department or unit of an organisation has operational responsibility for ensuring compliance for certain processing activity, it does not mean that this department or unit (rather than the organisation as a whole) becomes the controller.

> **Example**:
>
> The marketing department of Company ABC launches an advertising campaign to promote ABC's products. The marketing department decides the nature of campaign, the means to be used (e-mail, social media ...), which customers to target and what data to use in order to make the campaign as successful as possible. Even if the marketing department acted with considerable independence, Company ABC will in principle be considered as the controller seeing as the advertising campaign is launched by the company and takes place within the realm of its business activities and for its purposes.

19. In principle, any processing of personal data by employees which takes place within the realm of activities of an organisation may be presumed to take place under that organisation's control.[9] In exceptional circumstances, however, it may occur that an employee decides to use personal data for his or her own purposes, thereby unlawfully exceeding the authority that he or she was given. (e.g. to set up his own company or similar). It is therefore the organisation's duty as controller to make sure

[5] Article 29 Working Party Opinion 1/2010, WP 169, p. 9.
[6] See also the Opinion of Advocate General Mengozzi, in *Jehovah's witnesses*, C-25/17, ECLI:EU:C:2018:57, paragraph 68 ("*For the purposes of determining the 'controller' within the meaning of Directive 95/46, I am inclined to consider [....] that excessive formalism would make it easy to circumvent the provisions of Directive 95/46 and that, consequently, it is necessary to rely upon a more factual than formal analysis [...].*")
[7] CJEU, Case C-131/12, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, judgment of 13 May 2014, paragraph 34; CJEU, Case C-210/16, Wirtschaftsakademie Schleswig-Holstein, judgment of 5 June 2018, paragraph 28; CJEU, Case C-40/17, Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV, judgment of 29 July 2019, paragraph 66.
[8] For example, in its Judgment in *Jehovah's witnesses*, C-25/17, ECLI:EU:C:2018:551, paragraph 75, the CJEU considered that a religious community of Jehovah's witnesses acted as a controller, jointly with its individual members. Judgment in *Jehovah's witnesses*, C-25/17, ECLI:EU:C:2018:551, paragraph 75.
[9] Employees who have access to personal data within an organisation are generally not considered as "controllers" or "processors", but rather as "persons acting under the authority of the controller or of the processor" within the meaning of article 29 GDPR.

that there are adequate technical and organizational measures, including e.g. training and information to employees, to ensure compliance with the GDPR. [10]

2.1.2 "Determines"

20. The second building block of the controller concept refers to the controller's *influence* over the processing, by virtue of an *exercise of decision-making power*. A controller is a body that *decides* certain key elements about the processing. This controllership may be defined by law or may stem from an analysis of the factual elements or circumstances of the case. One should look at the specific processing operations in question and understand who determines them, by first considering the following questions: "*why is this processing taking place*?" and "*who decided that the processing should take place for a particular purpose?*".

Circumstances giving rise to control

21. Having said that the concept of controller is a functional concept, it is therefore based on a **factual rather than a formal analysis**. In order to facilitate the analysis, certain rules of thumb and practical presumptions may be used to guide and simplify the process. In most situations, the "determining body" can be easily and clearly identified by reference to certain legal and/or factual circumstances from which "influence" normally can be inferred, unless other elements indicate the contrary. Two categories of situations can be distinguished: (1) control stemming from *legal provisions*; and (2) control stemming from *factual influence*.

1) *Control stemming from legal provisions*

22. There are cases where control can be inferred from explicit legal competence e.g., when the controller or the specific criteria for its nomination are designated by national or Union law. Indeed, Article 4(7) states that "*where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.*" While Article 4(7) only refers to "the controller" in the singular form, the EDPB considers that it may also be possible for Union or Member State law to designate more than one controller, possibly even as joint controllers.

23. Where the controller has been specifically identified by law this will be determinative for establishing who is acting as controller. This presupposes that the legislator has designated as controller the entity that has a genuine ability to exercise control. In some countries, the national law provides that public authorities are responsible for processing of personal data within the context of their duties.

24. However, more commonly, rather than directly appointing the controller or setting out the criteria for its appointment, the law will establish a task or impose a duty on someone to collect and process certain data. In those cases, the purpose of the processing is often determined by the law. The controller will normally be the one designated by law for the realization of this purpose, this public task. For example, this would be the case where an entity which is entrusted with certain public tasks (e.g., social security) which cannot be fulfilled without collecting at least some personal data, sets up a database or register in order to fulfil those public tasks. In that case, the law, albeit indirectly, sets out who is the controller. More generally, the law may also impose an obligation on either public or private entities to retain or provide certain data. These entities would then normally be considered as controllers with respect to the processing that is necessary to execute this obligation.

[10] Article 24(1) GDPR.

Example: Legal provisions

The national law in Country A lays down an obligation for municipal authorities to provide social welfare benefits such as monthly payments to citizens depending on their financial situation. In order to carry out these payments, the municipal authority must collect and process data about the applicants' financial circumstances. Even though the law does not explicitly state that the municipal authorities are controllers for this processing, this follows implicitly from the legal provisions.

2) *Control stemming from factual influence*

25. In the absence of control arising from legal provisions, the qualification of a party as controller must be established on the basis of an assessment of the factual circumstances surrounding the processing. All relevant factual circumstances must be taken into account in order to reach a conclusion as to whether a particular entity exercises a determinative influence with respect to the processing of personal data in question.

26. The need for factual assessment also means that the role of a controller does not stem from the nature of an entity that is processing data but from its concrete activities in a specific context. In other words, the same entity may act at the same time as controller for certain processing operations and as processor for others, and the qualification as controller or processor has to be assessed with regard to each specific data processing activity.

27. In practice, certain processing activities can be considered as naturally attached to the role or activities of an entity ultimately entailing responsibilities from a data protection point of view. This can be due to more general legal provisions or an established legal practice in different areas (civil law, commercial law, labor law etc.). In this case, existing traditional roles and professional expertise that normally imply a certain responsibility will help in identifying the controller, for example: an employer in relation to processing personal data about his employees, a publisher processing personal data about its subscribers, or an association processing personal data about its members or contributors. When an entity engages in processing of personal data as part of its interactions with its own employees, customers or members, it will generally be the one who determines the purpose and means around the processing and is therefore acting as a controller within the meaning of the GDPR.

Example: Law firms

The company ABC hires a law firm to represent it in a dispute. In order to carry out this task, the law firm needs to process personal data related to the case. The reasons for processing the personal data is the law firm's mandate to represent the client in court. This mandate however is not specifically targeted to personal data processing. The law firm acts with a significant degree of independence, for example in deciding what information to use and how to use it, and there are no instructions from the client company regarding the personal data processing. The processing that the law firm carries out in order to fulfil the task as legal representative for the company is therefore linked to the functional role of the law firm so that it is to be regarded as controller for this processing.

Example: Telecom operators[11]:

[11] The EDPB considers that this example, previously included in Recital (47) of Directive 95/46/EC, remains relevant also under the GDPR.

Providing an electronic communications service such as an electronic mail service involves processing of personal data. The provider of such services will normally be considered a controller in respect of the processing of personal data that is necessary for the operation of the service as such (e.g., traffic and billing data). If the sole purpose and role of the provider is to enable the transmission of email messages, the provider will not be considered as the controller in respect of the personal data contained in the message itself. The controller in respect of any personal data contained inside the message will normally be considered to be the person from whom the message originates, rather than the service provider offering the transmission service.

28. In many cases, an assessment of the contractual terms between the different parties involved can facilitate the determination of which party (or parties) is acting as controller. Even if a contract is silent as to who is the controller, it may contain sufficient elements to infer who exercises a decision-making role with respect to the purposes and means of the processing. It may also be that the contract contains an explicit statement as to the identity of the controller. If there is no reason to doubt that this accurately reflects the reality, there is nothing against following the terms of the contract. However, the terms of a contract are not decisive in all circumstances, as this would simply allow parties to allocate responsibility as they see fit. It is not possible either to become a controller or to escape controller obligations simply by shaping the contract in a certain way where the factual circumstances say something else.

29. If one party in fact decides why and how personal data are processed that party will be a controller even if a contract says that it is a processor. Similarly, it is not because a commercial contract uses the term "subcontractor" that an entity shall be considered a processor from the perspective of data protection law.[12]

30. In line with the factual approach, the word "determines" means that the entity that actually exerts a decisive influence on the purposes and means of the processing is the controller. Normally, a processor agreement establishes who the determining party (controller) and the instructed party (processor) are. Even if the processor offers a service that is preliminary defined in a specific way, the controller has to be presented with a detailed description of the service and must make the final decision to actively approve the way the processing is carried out and request changes if necessary. Furthermore, the processor cannot at a later stage change the essential elements of the processing without the approval of the controller.

Example: standardised cloud storage service

A large cloud storage provider offers its customers the ability to store large volumes of personal data. The service is completely standardised, with customers having little or no ability to customise the service. The terms of the contract are determined and drawn up unilaterally by the cloud service provider, provided to the customer on a "take it or leave it basis". Company X decides to make use of the cloud provider to store personal data concerning its customers. Company X will still be considered a controller, given its decision to make use of this particular cloud service provider in order to process personal data for its purposes. Insofar as the cloud service provider does not process the personal data for its own purposes and stores the data solely on behalf of its customers and in accordance with instructions, the service provider will be considered as a processor.

[12] See e.g., Article 29 Data Protection Working Party, Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT), 22 November 2006, WP128, p. 11.

2.1.3 "Alone or jointly with others"

31. Article 4(7) recognizes that the "purposes and means" of the processing might be determined by more than one actor. It states that the controller is the actor who "alone or jointly with others" determines the purposes and means of the processing. This means that several different entities may act as controllers for the same processing, with each of them then being subject to the applicable data protection provisions. Correspondingly, an organisation can still be a controller even if it does not make all the decisions as to purposes and means. The criteria for joint controllership and the extent to which two or more actors jointly exercise control may take different forms, as clarified later on.[13]

2.1.4 "Purposes and means"

32. The fourth building block of the controller definition refers to the object of the controller's influence, namely the "purposes and means" of the processing. It represents the substantive part of the controller concept: what a party should determine in order to qualify as controller.

33. Dictionaries define "purpose" as "an anticipated outcome that is intended or that guides your planned actions" and "means" as "how a result is obtained or an end is achieved".

34. The GDPR establishes that data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Determination of the "purposes" of the processing and the "means" to achieve them is therefore particularly important.

35. Determining the purposes and the means amounts to deciding respectively the "why" and the "how" of the processing:[14] given a particular processing operation, the controller is the actor who has determined *why* the processing is taking place (i.e., "to what end"; or "what for") and *how* this objective shall be reached (i.e. which means shall be employed to attain the objective). A natural or legal person who exerts such influence over the processing of personal data, thereby participates in the determination of the purposes and means of that processing in accordance with the definition in Article 4(7) GDPR.[15]

36. The controller must decide on both purpose and means of the processing as described below. As a result, the controller cannot settle with only determining the purpose. It must also make decisions about the means of the processing. Conversely, the party acting as processor can never determine the purpose of the processing.

37. In practice, if a controller engages a processor to carry out the processing on its behalf, it often means that the processor shall be able to make certain decisions of its own on how to carry out the processing. The EDPB recognizes that some margin of manoeuvre may exist for the processor also to be able to make some decisions in relation to the processing. In this perspective, there is a need to provide guidance about which **level of influence** on the "why" and the "how" should entail the qualification of an entity as a controller and to what extent a processor may make decisions of its own.

38. When one entity clearly determines purposes and means, entrusting another entity with processing activities that amount to the execution of its detailed instructions, the situation is straightforward, and there is no doubt that the second entity should be regarded as a processor, whereas the first entity is the controller.

[13] See Part I, Section 3 ("Definition of joint controllers").
[14] See also the Opinion of Advocate General Bot in *Wirtschaftsakademie*, C-210/16, ECLI:EU:C:2017:796, paragraph 46.
[15] Judgment in *Jehovah's witnesses*, C-25/17, ECLI:EU:C:2018:551, paragraph 68.

Essential vs. non-essential means

39. The question is where to draw the line between decisions that are reserved to the controller and decisions that can be left to the discretion of the processor. Decisions on the purpose of the processing are clearly always for the controller to make.

40. As regards the determination of means, a distinction can be made between essential and non-essential means. "Essential means" are traditionally and inherently reserved to the controller. While non-essential means can also be determined by the processor, essential means are to be determined by the controller. "Essential means" are means that are closely linked to the purpose and the scope of the processing, such as the type of personal data which are processed ("*which data shall be processed?*"), the duration of the processing ("*for how long shall they be processed?*"), the categories of recipients ("*who shall have access to them?*") and the categories of data subjects ("*whose personal data are being processed?*"). Together with the purpose of processing, the essential means are also closely linked to the question of whether the processing is lawful, necessary and proportionate. "Non-essential means" concern more practical aspects of implementation, such as the choice for a particular type of hard- or software or the detailed security measures which may be left to the processor to decide on.

Example: Payroll administration

Employer A hires another company to administer the payment of salaries to its employees. Employer A gives clear instructions on who to pay, what amounts, by what date, by which bank, how long the data shall be stored, what data should be disclosed to the tax authority etc. In this case, the processing of data is carried out for Company A's purpose to pay salaries to its employees and the payroll administrator may not use the data for any purpose of its own. The way in which the payroll administrator should carry out the processing is in essence clearly and tightly defined. Nevertheless, the payroll administrator may decide on certain detailed matters around the processing such as which software to use, how to distribute access within its own organisation etc. This does not alter its role as processor as long as the administrator does not go against or beyond the instructions given by Company A.

Example: Bank payments

As part of the instructions from Employer A, the payroll administration transmits information to Bank B so that they can carry out the actual payment to the employees of Employer A. This activity includes processing of personal data by Bank B which it carries out for the purpose of performing banking activity. Within this activity, the bank decides independently from Employer A on which data that have to be processed to provide the service, for how long the data must be stored etc. Employer A cannot have any influence on the purpose and means of Bank B's processing of data. Bank B is therefore to be seen as a controller for this processing and the transmission of personal data from the payroll administration is to be regarded as a disclosure of information between two controllers, from Employer A to Bank B.

Example: Accountants

Employer A also hires Accounting firm C to carry out audits of their bookkeeping and therefore transfers data about financial transactions (including personal data) to C. Accounting firm C processes these data without detailed instructions from A. Accounting firm C decides itself, in accordance with legal provisions regulating the tasks of the auditing activities carried out by C, that the data it collects will only be processed for the purpose of auditing A and it determines what data it needs to have, which categories of persons that need to be registered, how long the data shall be kept and what technical means to use. Under these circumstances, Accounting firm C is to be regarded as a controller of its own when performing its auditing services for A. However, this assessment may be different depending on the level of instructions from A. In a situation where the law does not lay down specific obligations for the accounting firm and the client company provides very detailed instructions on the processing, the accounting firm would indeed be acting as a processor. A distinction could be made between a situation where the processing is - in accordance with the laws regulating this profession - done as part of the accounting firm's core activity and where the processing is a more limited, ancillary task that is carried out as part of the client company's activity.

Example: Hosting services

Employer A hires hosting service H to store encrypted data on H's servers. The hosting service H does not determine whether the data it hosts are personal data nor does it process data in any other way than storing it on its servers. As storage is one example of a personal data processing activity, the hosting service H is processing personal data on employer A's behalf and is therefore a processor. Employer A must provide the necessary instructions to H and a data processing agreement according to Article 28 must be concluded, requiring H to implement technical and organisational security measures. H must assist A in ensuring that the necessary security measures are taken and notify it in case of any personal data breach.

41. Even though decisions on non-essential means can be left to the processor, the controller must still stipulate certain elements in the processor agreement, such as – in relation to the security requirement, e.g. an instruction to take all measures required pursuant to Article 32 of the GDPR. The agreement must also state that the processor shall assist the controller in ensuring compliance with, for example, Article 32. In any event, the controller remains responsible for the implementation of appropriate technical and organisational measures to ensure and be able to demonstrate that the processing is performed in accordance with the Regulation (Article 24). In doing so, the controller must take into account the nature, scope, context and purposes of the processing as well as the risks for rights and freedoms of natural persons. For this reason, the controller must be fully informed about the means that are used so that it can take an informed decision in this regard. In order for the controller to be able to demonstrate the lawfulness of the processing, it is advisable to document at the minimum necessary technical and organisational measures in the contract or other legally binding instrument between the controller and the processor.

Example: Call centre

Company X decides to outsource a part of its customer service relations to a call centre. The call centre receives identifiable data about customer purchases, as well contact information. The call centre uses its own software and IT infrastructure to manage the personal data concerning Company X's customers. Company X signs a processor agreement with the provider of the call centre in accordance with Article 28 GDPR, after determining that the technical and organisational security measures proposed by the call centre are appropriate for the risks concerned and that the call centre will only process the personal data for the purposes of Company X and in accordance with its instructions. Company X does not provide any further instructions to the call centre as to specific software to be used nor any detailed instructions regarding the specific security measures to be implemented. In this example, Company X remains a controller, despite the fact that the call centre has determined certain non-essential means of the processing.

2.1.5 "Of the processing of personal data"

42. The purposes and means determined by the controller must relate to the "processing of personal data". Article 4(2) GDPR defines the processing of personal data as "*any operation or set of operations which is performed on personal data or on sets of personal data*". As a result, the concept of a controller can be linked either to a single processing operation or to a set of operations. In practice, this may mean that the control exercised by a particular entity may extend to the entirety of processing at issue but may also be limited to a particular stage in the processing.[16]

43. In practice, the processing of personal data involving several actors may be divided into several smaller processing operations for which each actor could be considered to determine the purpose and means individually. On the other hand, a sequence or set of processing operations involving several actors may also take place for the same purpose(s), in which case it is possible that the processing involves one or more joint controllers. In other words, it is possible that at "micro-level" the different processing operations of the chain appear as disconnected, as each of them may have a different purpose. However, it is necessary to double check whether at "macro-level" these processing operations should not be considered as a "set of operations" pursuing a joint purpose using jointly defined means.

44. Anyone who decides to process data must consider whether this includes personal data and, if so, what the obligations are according to the GDPR. An actor will be considered a "controller" even if it does not deliberately target personal data as such or has wrongfully assessed that it does not process personal data.

45. It is not necessary that the controller actually has access to the data that is being processed.[17] Someone who outsources a processing activity and in doing so, has a determinative influence on the purpose and (essential) means of the processing (e.g. by adjusting parameters of a service in such a way that it influences whose personal data shall be processed), is to be regarded as controller even though he or she will never have actual access to the data.

Example: Market research 1

Company ABC wishes to understand which types of consumers are most likely to be interested in its products and contracts a service provider, XYZ, to obtain the relevant information.

Company ABC instructs XYZ on what type of information it is interested in and provides a list of questions to be asked to those participating in the market research.

Company ABC receives only statistical information (e.g., identifying consumer trends per region) from XYZ and does not have access to the personal data itself. Nevertheless, Company ABC decided that the processing should take place, the processing is carried out for its purpose and its activity and it has provided XYZ with detailed instructions on what information to collect. Company ABC is therefore still to be considered a controller with respect of the processing of personal data that takes place in order to deliver the information it has requested. XYZ may only process the data for the purpose given by Company ABC and according to its detailed instructions and is therefore to be regarded as processor.

[16] Judgment in *Fashion ID*, C-40/17, ECLI:EU:C:2019:629, paragraph 74: "*(A)s the Advocate General noted, […] it appears that a natural or legal person may be a controller, within the meaning of Article 2(d) of Directive 95/46, jointly with others only in respect of operations involving the processing of personal data for which it determines jointly the purposes and means. By contrast, […] that natural or legal person cannot be considered to be a controller, within the meaning of that provision, in the context of operations that precede or are subsequent in the overall chain of processing for which that person does not determine either the purposes or the means*".
[17] Judgment in *Wirtschaftsakademie*, C-201/16, ECLI :EU :C :2018 :388, paragraph 38.

Example: Market research 2

Company ABC wishes to understand which types of consumers are most likely to be interested in its products. Service provider XYZ is a market research agency which has collected information about consumer interests through a variety of questionnaires which pertain to a wide variety of products and services. Service provider XYZ has collected and analysed this data independently, according to its own methodology without receiving any instructions from Company ABC. To answer Company ABC's request, service provider XYZ will generate statistical information, but does so without receiving any further instructions about which personal data should be processed or how to process it in order to generate these statistics. In this example, service provider XYZ acts as the sole controller, processing personal data for market research purposes, autonomously determining the means for doing so. Company ABC does not have any particular role or responsibility under data protection law in relation to these processing activities, as Company ABC receives anonymised statistics and is not involved in determining the purposes and means of the processing.

3 DEFINITION OF JOINT CONTROLLERS

3.1 Definition of joint controllers

46. The qualification as joint controllers may arise where more than one actor is involved in the processing.

47. While the concept is not new and already existed under Directive 95/46/EC, the GDPR, in its Article 26, introduces specific rules for joint controllers and sets a framework to govern their relationship. In addition, the Court of Justice of the European Union (CJEU) in recent rulings has brought clarifications on this concept and its implications.[18]

48. As further elaborated in Part II, section 2, the qualification of joint controllers will mainly have consequences in terms of allocation of obligations for compliance with data protection rules and in particular with respect to the rights of individuals.

49. In this perspective, the following section aims to provide guidance on the concept of joint controllers in accordance with the GDPR and the CJEU case law to assist entities in determining where they may be acting as joint controllers and applying the concept in practice.

3.2 Existence of joint controllership

3.2.1 General considerations

50. The definition of a controller in Article 4 (7) GDPR forms the starting point for determining joint controllership. The considerations in this section are thus directly related to and supplement the

[18] See in particular, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie*, (C-210/16), *Tietosuojavaltuutettu v Jehovan todistajat — uskonnollinen yhdyskunta* (C-25/17), *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV* (C-40/17). To be noted that while these judgments were issued by the CJEU on the interpretation of the concept of joint controllers under Directive 95/46/CE, they remain valid in the context of the GDPR, given that the elements determining this concept under the GDPR remain the same as under the Directive.

considerations in the section on the concept of controller. As a consequence, the assessment of joint controllership should mirror the assessment of "single" control developed above.

51. Article 26 GDPR, which reflects the definition in Article 4 (7) GDPR, provides that *"[w]here two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers."* In broad terms, joint controllership exists with regard to a specific processing activity when different parties determine *jointly* the purpose and means of this processing activity. Therefore, assessing the existence of joint controllers requires examining whether the determination of purposes and means that characterize a controller are decided by more than one party. "Jointly" must be interpreted as meaning "together with" or "not alone", in different forms and combinations, as explained below.

52. The assessment of joint controllership should be carried out on a factual, rather than a formal, analysis of the actual influence on the purposes and means of the processing. All existing or envisaged arrangements should be checked against the factual circumstances regarding the relationship between the parties. A merely formal criterion would not be sufficient for at least two reasons: in some cases, the formal appointment of a joint controller - laid down for example by law or in a contract - would be absent; in other cases, it may be that the formal appointment does not reflect the reality of the arrangements, by formally entrusting the role of controller to an entity which actually is not in the position to "determine" the purposes and means of the processing.

53. Not all processing involving several entities give rise to joint controllership. The overarching criterion for joint controllership to exist is the **joint participation of two or more entities in the determination of the purposes and means** of a processing. More specifically, joint participation needs to include the determination of purposes on the one hand and the determination of means on the other hand. If each of these elements are determined by all entities concerned, they should be considered as joint controllers of the processing at issue.

3.2.2 Assessment of joint participation

54. Joint participation in the determination of purposes and means implies that more than one entity have a decisive influence over whether and how the processing takes place. In practice, joint participation can take several different forms. For example, joint participation can take the form of a **common decision** taken by two or more entities or result from **converging decisions** by two or more entities regarding the purposes and essential means.

55. Joint participation through a *common decision* means deciding together and involves a common intention in accordance with the most common understanding of the term "jointly" referred to in Article 26 of the GDPR.

The situation of joint participation through *converging decisions* results more particularly from the case law of the CJEU on the concept of joint controllers. Decisions can be considered as converging on purposes and means **if they complement each other and are necessary for the processing to take place in such manner that they have a tangible impact on the determination of the purposes and means of the processing**. It should be highlighted that the notion of converging decisions needs to be considered in relation to the purposes and means of the processing but not other aspects of the commercial relationship between the parties.[19] As such, an important criterion to identify converging decisions in this context **is whether the processing would not be possible without both parties' participation in the purposes and means in the sense that the processing by each party is inseparable, i.e. inextricably linked.** The situation of joint controllers acting on the basis of converging decisions should however be distinguished from the case of a processor, since the latter – while participating in the performance of a processing – does not process the data for its own purposes but carries out the processing on behalf of the controller.

[19] Indeed, all commercial arrangements involve converging decisions as part of the process by which an agreement is reached.

56. The fact that one of the parties does not have access to personal data processed is not sufficient to exclude joint controllership.[20] For example, in *Jehovah's Witnesses*, the CJEU considered that a religious community must be considered a controller, jointly with its members who engage in preaching, of the processing of personal data carried out by the latter in the context of door-to-door preaching.[21] The CJEU considered that it was not necessary that the community had access to the data in question, or to establish that that community had given its members written guidelines or instructions in relation to the data processing.[22] The community participated in the determination of purposes and means by organising and coordinating the activities of its members, which helped to achieve the objective of the Jehovah's Witnesses community.[23] In addition, the community had knowledge on a general level of the fact that such processing was carried out in order to spread its faith.[24]

57. It is also important to underline, as clarified by the CJEU, that an entity will be considered as joint controller with the other(s) only in respect of those operations for which it determines, jointly with others, the means and the purposes of the same data processing in particular in case of converging decisions. If one of these entities decides alone the purposes and means of operations that precede or are subsequent in the chain of processing, this entity must be considered as the sole controller of this preceding or subsequent operation.[25]

58. The existence of joint responsibility does not necessarily imply equal responsibility of the various operators involved in the processing of personal data. On the contrary, the CJEU has clarified that those operators may be involved at different stages of that processing and to different degrees so that the level of responsibility of each of them must be assessed with regard to all the relevant circumstances of the particular case.

3.2.2.1 Jointly determined purpose(s)

59. Joint controllership exists when entities involved in the same processing carry out the processing for jointly defined purposes. This will be the case if the entities involved process the data for the same, or common, purposes.

60. In addition, when the entities do not have the same purpose for the processing, joint controllership may also, in light of the CJEU case law, be established when the entities involved pursue purposes which are closely linked or complementary. Such may be the case, for example, when there is a mutual benefit arising from the same processing operation, provided that each of the entities involved participates in the determination of the purposes and means of the relevant processing operation. However, the notion of mutual benefit is not decisive and can only be an indication.. In *Fashion ID*, for example, the CJEU clarified that a website operator participates in the determination of the purposes

[20] Judgment in *Wirtschaftsakademie*, C-210/16, ECLI:EU:C:2018:388, paragraph 38.
[21] Judgment in *Jehovah's witnesses*, C-25/17, ECLI:EU:C:2018:551, paragraph 75.
[22] Ibid.
[23] Ibid, paragraph 71.
[24] Ibid.
[25] Judgment in *Fashion ID*, C-40/17, ECLI:EU:2018:1039, paragraph 74 *"By contrast, and without prejudice to any civil liability provided for in national law in this respect, that natural or legal person cannot be considered to be a controller, within the meaning of that provision, in the context of operations that precede or are subsequent in the overall chain of processing for which that person does not determine either the purposes or the means"*.

(and means) of the processing by embedding a social plug-in on a website in order to optimize the publicity of its goods by making them more visible on the social network. The CJEU considered that the processing operations at issue were performed in the economic interests of both the website operator and the provider of the social plug-in.[26]

61. Likewise, as noted by the CJEU in *Wirtschaftsakademie*, the processing of personal data through statistics of visitors to a fan page is intended to enable Facebook to improve its system of advertising transmitted via its network and to enable the administrator of the fan page to obtain statistics to manage the promotion of its activity.[27] Each entity in this case pursues its own interest but both parties participate in the determination of the purposes (and means) of the processing of personal data as regards the visitors to the fan page.[28]

62. In this respect, it is important to highlight that the mere existence of a mutual benefit (for ex. commercial) arising from a processing activity does not give rise to joint controllership. If the entity involved in the processing does not pursue any purpose(s) of its own in relation to the processing activity, but is merely being paid for services rendered, it is acting as a processor rather than as a joint controller.

3.2.2.2 Jointly determined means

63. Joint controllership also requires that two or more entities have exerted influence over the means of the processing. This does not mean that, for joint controllership to exist, each entity involved needs in all cases to determine all of the means. Indeed, as clarified by the CJEU, different entities may be involved at different stages of that processing and to different degrees. Different joint controllers may therefore define the means of the processing to a different extent, depending on who is effectively in a position to do so.

64. It may also be the case that one of the entities involved provides the means of the processing and makes it available for personal data processing activities by other entities. The entity who decides to make use of those means so that personal data can be processed for a particular purpose also participates in the determination of the means of the processing.

65. This scenario can notably arise in case of platforms, standardised tools, or other infrastructure allowing the parties to process the same personal data and which have been set up in a certain way by one of the parties to be used by others that can also decide how to set it up.[29] The use of an already existing technical system does not exclude joint controllership when users of the system can decide on the processing of personal data to be performed in this context.

66. As an example of this, the CJEU held in *Wirtschaftsakademie* that the administrator of a fan page hosted on Facebook, by defining parameters based on its target audience and the objectives of managing and promoting its activities, must be regarded as taking part in the determination of the means of the processing of personal data related to the visitors of its fan page.

67. Furthermore, the choice made by an entity to use for its own purposes a tool or other system developed by another entity, allowing the processing of personal data, will likely amount to a joint decision on the means of that processing by those entities. This follows from the Fashion ID case where

[26] Judgment in *Fashion ID*, C-40/17, ECLI:EU:2018:1039, paragraph 80.
[27] Judgment in *Wirtschaftsakademie*, C-210/16, ECLI:EU:C:2018:388, paragraph 34.
[28] Judgment in *Wirtschaftsakademie*, C-210/16, ECLI:EU:C:2018:388, paragraph 39.
[29] The provider of the system can be a joint controller if the criteria mentioned above are met, i.e. if the provider participates in the determination of purposes and means. Otherwise, the provider should be considered as a processor.

the CJEU concluded, that by embedding on its website the Facebook Like button made available by Facebook to website operators, Fashion ID has exerted a decisive influence in respect of the operations involving the collection and transmission of the personal data of the visitors of its website to Facebook and had thus jointly determined with Facebook the means of that processing.[30]

68. It is important to underline that **the use of a common data processing system or infrastructure will not in all cases lead to qualify the parties involved as joint controllers,** in particular where the processing they carry out is separable and could be performed by one party without intervention from the other or where the provider is a processor in the absence of any purpose of its own (the existence of a mere commercial benefit for the parties involved is not sufficient to qualify as a purpose of processing).

Example: Travel agency

A travel agency sends personal data of its customers to the airline and a chain of hotels, with a view to making reservations for a travel package. The airline and the hotel confirm the availability of the seats and rooms requested. The travel agency issues the travel documents and vouchers for its customers. Each of the actors processes the data for carrying out their own activities and using their own means. In this case, the travel agency, the airline and the hotel are three different data controllers processing the data for their own and separate purposes and there is no joint controllership.

The travel agency, the hotel chain and the airline then decide to participate jointly in setting up an internet-based common platform for the common purpose of providing package travel deals. They agree on the essential means to be used, such as which data will be stored, how reservations will be allocated and confirmed, and who can have access to the information stored. Furthermore, they decide to share the data of their customers in order to carry out joint marketing actions. In this case, the travel agency, the airline and the hotel chain, jointly determine why and how personal data of their respective customers are processed and will therefore be joint controllers with regard to the processing operations relating to the common internet-based booking platform and the joint marketing actions. However, each of them would still retain sole control with regard to other processing activities outside the internet-based common platform.

Example: Research project by institutes

Several research institutes decide to participate in a specific joint research project and to use to that end the existing platform of one of the institutes involved in the project. Each institute feeds personal data it already holds into the platform for the purpose of the joint research and uses the data provided by others through the platform for carrying out the research. In this case, all institutes qualify as joint controllers for the personal data processing that is done by storing and disclosing information from this platform since they have decided together the purpose of the processing and the means to be used (the existing platform). Each of the institutes however is a separate controller for any other processing that may be carried out outside the platform for their respective purposes.

Example: Marketing operation

Companies A and B have launched a co-branded product C and wish to organise an event to promote this product. To that end, they decide to share data from their respective clients and prospects

[30] Judgment in Fashion ID, C-40/17, ECLI:EU:2018:1039, paragraphs 77-79.

database and decide on the list of invitees to the event on this basis. They also agree on the modalities for sending the invitations to the event, how to collect feedback during the event and follow-up marketing actions. Companies A and B can be considered as joint controllers for the processing of personal data related to the organisation of the promotional event as they decide together on the jointly defined purpose and essential means of the data processing in this context.

Example: Clinical Trials[31]

A health care provider (the investigator) and a university (the sponsor) decide to launch together a clinical trial with the same purpose. They collaborate together to the drafting of the study protocol (i.e. purpose, methodology/design of the study, data to be collected, subject exclusion/inclusion criteria, database reuse (where relevant) etc.). They may be considered as joint controllers, for this clinical trial as they jointly determine and agree on the same purpose and the essential means of the processing. The collection of personal data from the medical record of the patient for the purpose of research is to be distinguished from the storage and use of the same data for the purpose of patient care, for which the health care provider remains the controller.

In the event that the investigator does not participate to the drafting of the protocol (he just accepts the protocol already elaborated by the sponsor), and the protocol is only designed by the sponsor, the investigator should be considered as a processor and the sponsor as the controller for this clinical trial.

Example: Headhunters

Company X helps Company Y in recruiting new staff- with its famous value-added service "global matchz". Company X looks for suitable candidates both among the CVs received directly by Company Y and those it already has in its own database. Such database is created and managed by Company X on its own. This ensures that Company X enhances the matching between job offers and job seekers, thus increasing its revenues. Even though they have not formally taken a decision together, Companies X and Y jointly participate to the processing with the purpose of finding suitable candidates based on converging decisions: the decision to create and manage the service "global matchz" for Company X and the decision of Company Y to enrich the database with the CVs it directly receives. Such decisions complement each other, are inseparable and necessary for the processing of finding suitable candidates to take place. Therefore, in this particular case they should be considered as joint controllers of such processing. However, Company X is the sole controller of the processing necessary to manage its database and Company Y is the sole controller of the subsequent hiring processing for its own purpose (organisation of interviews, conclusion of the contract and management of HR data).

Example: Analysis of health data

Company ABC, the developer of a blood pressure monitoring app and Company XYZ, a provider of apps for medical professionals, both wish to examine how blood pressure changes can help predict certain diseases. The companies decide to set up a joint project and reach out to Hospital DEF to become involved as well.

The personal data that will be processed in this project consists of personal data which Company ABC, Hospital DEF and Company XYZ are separately processing as individual controllers. The decision to process this data to assess blood pressure changes is taken jointly by the three actors. Company ABC, Hospital DEF and Company XYZ have jointly determined the purposes of processing. Company XYZ takes the initiative to propose the essential means of processing. Both Company ABC and the Hospital DEF accept these essential means after they as well were involved in developing some of the features of the app so that the results can be sufficiently used by them. The three organizations thus agree on having a common purpose for the processing which is the assessment of how blood pressure changes can help predict certain diseases. Once the research is completed, Company ABC, Hospital DEF and Company XYZ may benefit from the assessment by using its results in their own activities. For all these reasons, they qualify as joint controllers for this specific joint processing.

If Company XYZ had been simply asked by the others to perform this assessment without having any purpose of their own and merely been processing data on behalf of the others, Company XYZ would qualify as a processor even if it was entrusted with the determination of the non-essential means.

[31] The EDPB plans to provide further guidance in relation to clinical trials in the context of its forthcoming Guidelines on processing of personal data for medical and scientific research purposes.

3.2.3 Situations where there is no joint controllership

69. The fact that several actors are involved in the same processing does not mean that they are necessarily acting as joint controllers of such processing. Not all kind of partnerships, cooperation or collaboration imply qualification of joint controllers as such qualification requires a case-by-case analysis of each processing at stake and the precise role of each entity with respect to each processing. The cases below provide non-exhaustive examples of situations where there is no joint controllership.

70. For example, the exchange of the same data or set of data between two entities without jointly determined purposes or jointly determined means of processing should be considered as a transmission of data between separate controllers.

Example: Transmission of employee data to tax authorities

A company collects and processes personal data of its employees with the purpose of managing salaries, health insurances, etc. A law imposes an obligation on the company to send all data concerning salaries to the tax authorities, with a view to reinforce fiscal control.

In this case, even though both the company and the tax authorities process the same data concerning salaries, the lack of jointly determined purposes and means with regard to this data processing will result in qualifying the two entities as two separate data controllers.

71. Joint controllership may also be excluded in a situation where several entities use a shared database or a common infrastructure, if each entity independently determines its own purposes.

Example: Marketing operations in a group of companies using a shared database:

A group of companies uses the same database for the management of clients and prospects. Such database is hosted on the servers of the mother company who is therefore a processor of the companies with respect to the storage of the data. Each entity of the group enters the data of its own clients and prospects and processes such data for its own purposes only. Also, each entity decides independently on the access, the retention periods, the correction or deletion of their clients and prospects' data. They cannot access or use each other's data. The mere fact that these companies use a shared group database does not as such entail joint controllership. Under these circumstances, each company is thus a separate controller.

Example: Independent controllers when using a shared infrastructure

Company XYZ hosts a database and makes it available to other companies to process and host personal data about their employees. Company XYZ is a processor in relation to the processing and storage of other companies' employees as these operations are performed on behalf and according to the instructions of these other companies. In addition, the other companies process the data without any involvement from Company XYZ and for purposes which are not in any way shared by Company XYZ.

72. Also, there can be situations where various actors successively process the same personal data in a chain of operations, each of these actors having an independent purpose and independent means in their part of the chain. In the absence of joint participation in the determination of the purposes and means of the same processing operation or set of operations, joint controllership has to be excluded and the various actors must be regarded as successive independent controllers.

Example: Statistical analysis for a task of public interest

A public authority (Authority A) has the legal task of making relevant analysis and statistics on how the country's employment rate develops. To do that, many other public entities are legally bound to disclose specific data to Authority A. Authority A decides to use a specific system to process the data, including collection. This also means that the other units are obligated to use the system for their disclosure of data. In this case, without prejudice to any attribution of roles by law, Authority A will be the only controller of the processing for the purpose of analysis and statistics of the employment rate processed in the system, because Authority A determines the purpose for the processing, and has decided how the processing will be organised. Of course, the other public entities, as controllers for their own processing activities, are responsible for ensuring the accuracy of the data they previously processed, which they then disclose to Authority A.

4 DEFINITION OF PROCESSOR

73. A processor is defined in Article 4 (8) as a natural or legal person, public authority, agency or another body, which processes personal data on behalf of the controller. Similar to the definition of controller, the definition of processor envisages a broad range of actors - it can be "*a natural or legal person, public authority, agency or other body*". This means that there is in principle no limitation as to which type of actor might assume the role of a processor. It might be an organisation, but it might also be an individual.

74. The GDPR lays down obligations directly applicable specifically to processors as further specified in Part II section 1 of these guidelines. A processor can be held liable or fined in case of failure to comply with such obligations or in case it acts outside or contrary to the lawful instructions of the controller.

75. Processing of personal data can involve multiple processors. For example, a controller may itself choose to directly engage multiple processors, by involving different processors at separate stages of the processing (multiple processors). A controller might also decide to engage one processor, who in turn - with the authorisation of the controller - engages one or more other processors ("sub processor(s)"). The processing activity entrusted to the processor may be limited to a very specific task or context or may be more general and extended.

76. Two basic conditions for qualifying as processor are:

    a) being *a separate entity* in relation to the controller and

    b) processing personal data *on the controller's behalf*.

77. *A separate entity* means that the controller decides to delegate all or part of the processing activities to an external organisation. Within a group of companies, one company can be a processor to another company acting as controller, as both companies are separate entities. On the other hand, a department within a company cannot be a processor to another department within the same entity.

78. If the controller decides to process data itself, using its own resources within its organisation, for example through its own staff, this is not a processor situation. Employees and other persons that are acting under the direct authority of the controller, such as temporarily employed staff, are not to be seen as processors since they will process personal data as a part of the controller's entity. In accordance with Article 29, they are also bound by the controller's instructions.

79. *Processing personal data on the controller's behalf* firstly requires that the separate entity processes personal data for the benefit of the controller. In Article 4(2), processing is defined as a concept including a wide array of operations ranging from collection, storage and consultation to use, dissemination or otherwise making available and destruction.. The concept of "processing" is further described above under 2.1.5.

80. Secondly, the processing must be done on behalf of a controller but otherwise than under its direct authority or control. Acting "on behalf of" means serving someone else's interest and recalls the legal concept of "delegation". In the case of data protection law, a processor is called to implement the instructions given by the controller at least with regard to the purpose of the processing and the essential elements of the means. The lawfulness of the processing according to Article 6, and if relevant Article 9, of the Regulation will be derived from the controller's activity and the processor must not process the data otherwise than according to the controller's instructions. Even so, as described above, the controller's instructions may still leave a certain degree of discretion about how to best serve the controller's interests, allowing the processor to choose the most suitable technical and organisational means.[32]

81. Acting "on behalf of" also means that the processor may not carry out processing for its own purpose(s). As provided in Article 28(10), a processor infringes the GDPR by going beyond the controller's instructions and starting to determine its own purposes and means of processing. The processor will be considered a controller in respect of that processing and may be subject to sanctions for going beyond the controller's instructions.

Example: Service provider referred to as data processor but acting as controller

Service provider MarketinZ provides promotional advertisement and direct marketing services to various companies. Company GoodProductZ concludes a contract with MarketinZ, according to which the latter company provides commercial advertising for GoodProductZ customers and is referred to as data processor. However, MarketinZ decides to use GoodProducts customer database also for other purposes than advertising for GoodProducts, such as developing their own business activity. The decision to add an additional purpose to the one for which the personal data were transferred converts MarketinZ into a data controller for this set of processing operations and their processing for this purpose would constitute an infringement of the GDPR.

82. The EDPB recalls that not every service provider that processes personal data in the course of delivering a service is a "processor" within the meaning of the GDPR. The role of a processor does not stem from the nature of an entity that is processing data but from its concrete activities in a specific context. In other words, the same entity may act at the same time as a controller for certain processing

[32] See Part I, sub-section 2.1.4 describing the distinction between essential and non-essential means.

operations and as a processor for others, and the qualification as controller or processor has to be assessed with regard to specific sets of data or operations. The nature of the service will determine whether the processing activity amounts to processing of personal data on behalf of the controller within the meaning of the GDPR. In practice, where the provided service is not specifically targeted at processing personal data or where such processing does not constitute a key element of the service, the service provider may be in a position to independently determine the purposes and means of that processing which is required in order to provide the service. In that situation, the service provider is to be seen as a separate controller and not as a processor.[33] A case-by-case analysis remains necessary, however, in order to ascertain the degree of influence each entity effectively has in determining the purposes and means of the processing.

Example: Taxi service

A taxi service offers an online platform which allows companies to book a taxi to transport employees or guests to and from the airport. When booking a taxi, Company ABC specifies the name of the employee that should be picked up from the airport so the driver can confirm the employee's identity at the moment of pick-up. In this case, the taxi service processes personal data of the employee as part of its service to Company ABC, but the processing as such is not the target of the service. The taxi service has designed the online booking platform as part of developing its own business activity to provide transportation services, without any instructions from Company ABC. The taxi service also independently determines the categories of data it collects and how long it retains. The taxi service therefore acts as a controller in its own right, notwithstanding the fact that the processing takes place following a request for service from Company ABC.

83. The EDPB notes that a service provider may still be acting as a processor even if the processing of personal data is not the main or primary object of the service, provided that the customer of the service still determines the purposes and means of the processing in practice. When considering whether or not to entrust the processing of personal data to a particular service provider, controllers should carefully assess whether the service provider in question allows them to exercise a sufficient degree of control, taking into account the nature, scope, context and purposes of processing as well as the potential risks for data subjects.

Example: Call center

Company X outsources its client support to Company Y who provides a call center in order to help Company X's clients with their questions. The client support service means that Company Y has to have access to Company X client data bases. Company Y can only access data in order to provide the support that Company X has procured and they cannot process data for any other purposes than the ones stated by Company X. Company Y is to be seen as a personal data processor and a processor agreement must be concluded between Company X and Y.

Example: General IT support

Company Z hires an IT service provider to perform general support on its IT systems which include a vast amount of personal data. The access to personal data is not the main object of the support service but it is inevitable that the IT service provider systematically has access to personal data when performing the service. Company Z therefore concludes that the IT service provider - being a separate company and inevitably being required to process personal data even though this is not the main objective of the service – is to be regarded as a processor. A processor agreement is therefore concluded with the IT service provider.

Example: IT-consultant fixing a software bug

Company ABC hires an IT-specialist from another company to fix a bug in a software that is being used by the company. The IT-consultant is not hired to process personal data, and Company ABC determines that any access to personal data will be purely incidental and therefore very limited in practice. ABC therefore concludes that the IT-specialist is not a processor (nor a controller in its own right) and that Company ABC will take appropriate measures according to Article 32 of the GDPR in order to prevent the IT-consultant from processing personal data in an unauthorised manner.

84. As stated above, nothing prevents the processor from offering a preliminarily defined service but the controller must make the final decision to actively approve the way the processing is carried out, at least insofar as concerns the essential means of the processing. As stated above, a processor has a margin of manoeuvre as regards non-essential means, see above under sub-section 2.1.4.

Example: Cloud service provider

A municipality has decided to use a cloud service provider for handling information in its school and education services. The cloud service provides messaging services, videoconferences, storage of documents, calendar management, word processing etc. and will entail processing of personal data about school children and teachers. The cloud service provider has offered a standardized service that is offered worldwide. The municipality however must make sure that the agreement in place complies with Article 28(3) of the GDPR, that the personal data of which it is controller are processed for the municipality's purposes only. It must also make sure that their specific instructions on storage periods, deletion of data etc. are respected by the cloud service provider regardless of what is generally offered in the standardized service.

5 DEFINITION OF THIRD PARTY/RECIPIENT

85. The Regulation not only defines the concepts of controller and processor but also the concepts of recipient and third party. As opposed to the concepts of controller and processor, the Regulation does not lay down specific obligations or responsibilities for recipients and third parties. These can be said to be relative concepts in the sense that they describe a relation to a controller or processor from a specific perspective, e.g. a controller or processor discloses data to a recipient. A recipient of personal data and a third party may well simultaneously be regarded as a controller or processor from other perspectives. For example, entities that are to be seen as recipients or third parties from one perspective, are controllers for the processing for which they determine the purpose and means.

Third party

86. Article 4(10) defines a "*third party*" as a natural or legal person, public authority, agency or body other than

- the data subject,
- the controller,
- the processor and

[33] See also Recital 81 of the GDPR, which refers to "entrusting a processor processing activities", indicating that the processing activity as such is an important part of the decision of the controller to ask a processor to process personal data on its behalf.

- persons who, under the direct authority of the controller or processor, are authorised to process personal data.

87. The definition generally corresponds to the previous definition of "*third party*" in Directive 95/46/EC.

88. Whereas the terms "*personal data*", "*data subject*", "*controller*" and "*processor*" are defined in the Regulation, the concept of "*persons who, under the direct authority of the controller or processor, are authorised to process personal data*" is not. It is, however, generally understood as referring to persons that belong to the legal entity of the controller or processor (an employee or a role highly comparable to that of employees, e.g. interim staff provided via a temporary employment agency) but only insofar as they are authorized to process personal data. An employee etc. who obtains access to data that he or she is not authorised to access and for other purposes than that of the employer does not fall within this category. Instead, this employee should be considered as a third party vis-à-vis the processing undertaken by the employer. Insofar as the employee processes personal data for his or her own purposes, distinct from those of his or her employer, he or she will then be considered a controller and take on all the resulting consequences and liabilities in terms of personal data processing.[34]

89. A third party thus refers to someone who, in the specific situation at hand, is not a data subject, a controller, a processor or an employee. For example, the controller may hire a processor and instruct it to transfer personal data to a third party. This third party will then be considered a controller in its own right for the processing that it carries out for its own purposes. It should be noted that, within a group of companies, a company other than the controller or the processor is a third party, even though it belongs to the same group as the company who acts as controller or processor.

Example: Cleaning services

Company A concludes a contract with a cleaning service company to clean its offices. The cleaners are not supposed to access or otherwise process personal data. Even though they may occasionally come across such data when moving around in the office, they can carry out their task without accessing data and they are contractually prohibited to access or otherwise process personal data that Company A keeps as controller. The cleaners are not employed by Company A nor are they seen as being under the direct authority of that company. There is no intention to engage the cleaning service company or its employees to process personal data on Company A's behalf. The cleaning service company and its employees are therefore to be seen as a third party and the controller must make sure that there are adequate security measures to prevent that they have access to data and lay down a confidentiality duty in case they should accidentally come across personal data.

Example: Company groups – parent company and subsidiaries

Companies X and Y form part of the Group Z. Companies X and Y both process data about their respective employees for employee administration purposes. At one point, the parent company ZZ decides to request employee data from all subsidiaries in order to produce group wide statistics. When transferring data from companies X and Y to ZZ, the latter is to be regarded as a third party regardless of the fact that all companies are part of the same group. Company ZZ will be regarded as controller for its processing of the data for statistical purposes.

[34] The employer (as original controller) could nevertheless retain some responsibility in case the new processing occurred because of a lack of adequate security measures.

Recipient

90. Article 4(9) defines a "*recipient*" as a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. Public authorities are however not to be seen as recipients when they receive personal data in the framework of a particular inquiry in accordance with Union or Member State law (e.g. tax and customs authorities, financial investigation units etc.)[35]

91. The definition generally corresponds to the previous definition of "*recipient*" in Directive 95/46/EC.

92. The definition covers anyone who receives personal data, whether they are a third party or not. For example, when a controller sends personal data to another entity, either a processor or a third party, this entity is a recipient. A third party recipient shall be considered a controller for any processing that it carries out for its own purpose(s) after it receives the data.

Example: Disclosure of data between companies

The travel agency ExploreMore arranges travels on request from its individual customers. Within this service, they send the customers' personal data to airlines, hotels and organisations of excursions in order for them to carry out their respective services. ExploreMore, the hotels, airlines and excursion providers are each to be seen as controllers for the processing that they carry out within their respective services. There is no controller-processor relation. However, the airlines, hotels and excursion providers are to be seen as recipients when receiving the personal data from ExploreMore.

PART II – CONSEQUENCES OF ATTRIBUTING DIFFERENT ROLES

1 RELATIONSHIP BETWEEN CONTROLLER AND PROCESSOR

93. A distinct new feature in the GDPR are the provisions that impose obligations directly upon processors. For example, a processor must ensure that persons authorised to process the personal data have committed themselves to confidentiality (Article 28(3)); a processor must maintain a record of all categories of processing activities (Article 30(2)) and must implement appropriate technical and organisational measures (Article 32). A processor must also designate a data protection officer under certain conditions (Article 37) and has a duty to notify the controller without undue delay after becoming aware of a personal data breach (Article 33(2)). Furthermore, the rules on transfers of data to third countries (Chapter V) apply to processors as well as controllers. In this regard, the EDPB considers that Article 28(3) GDPR, while mandating a specific content for the necessary contract between controller and processor, imposes direct obligations upon processors, including the duty to assist the controller in ensuring compliance.[36]

1.1 Choice of the processor

94. The controller has the **duty to use "only processors providing sufficient guarantees** to implement appropriate technical and organisational measures", so that processing meets the requirements of the

[35] See also Recital 31 of the GDPR

[36] For instance, the processor should assist the controller, where necessary and upon request, in ensuring compliance with obligations relating to data protection impact assessments (Recital 95 GDPR). This needs to be reflected in the contract between the controller and the processor pursuant to Article 28(3)(f) GDPR.

GDPR - including for the security of processing - and ensures the protection of data subject rights.[37] The controller is therefore responsible for assessing the sufficiency of the guarantees provided by the processor and should be able to prove that it has taken all of the elements provided in the GDPR into serious consideration.

95. The guarantees "provided" by the processor are those that the processor is able to **demonstrate to the satisfaction of the controller**, as those are the only ones that can effectively be taken into account by the controller when assessing compliance with its obligations. Often this will require an exchange of relevant documentation (e.g. privacy policy, terms of service, record of processing activities, records management policy, information security policy, reports of external data protection audits, recognised international certifications, like ISO 27000 series).

96. The controller's assessment of whether the guarantees are sufficient is a form of risk assessment, which will greatly depend on the type of processing entrusted to the processor and needs to be made on a case-by-case basis, taking into account the nature, scope, context and purposes of processing as well as the risks for the rights and freedoms of natural persons. As a consequence, the EDPB cannot provide an exhaustive list of the documents or actions that the processor needs to show or demonstrate in any given scenario, as this largely depends on the specific circumstances of the processing.

97. The following elements[38] should be taken into account by the controller in order to assess the sufficiency of the guarantees: the processor's **expert knowledge** (e.g. technical expertise with regard to security measures and data breaches); the processor's **reliability**; the processor's **resources**. The reputation of the processor on the market may also be a relevant factor for controllers to consider.

98. Furthermore, the adherence to an approved code of conduct or certification mechanism can be used as an element by which sufficient guarantees can be demonstrated.[39] The processors are therefore advised to inform the controller as to this circumstance, as well as to any change in such adherence.

99. The obligation to use only processors "providing sufficient guarantees" contained in Article 28(1) GDPR is a continuous obligation. It does not end at the moment where the controller and processor conclude a contract or other legal act. Rather the controller should, at appropriate intervals, verify the processor's guarantees, including through audits and inspections where appropriate.[40]

1.2 Form of the contract or other legal act

100. Any processing of personal data by a processor must be governed by a contract or other legal act under EU or Member State law between the controller and the processor, as required by Article 28(3) GDPR.

101. Such legal act must be **in writing, including in electronic form**.[41] Therefore, non-written agreements (regardless of how thorough or effective they are) cannot be considered sufficient to meet the requirements laid down by Article 28 GDPR. To avoid any difficulties in demonstrating that the contract or other legal act is actually in force, the EDPB recommends ensuring that the necessary signatures are included in the legal act, in line with applicable law (e.g. contract law).

[37] Article 28(1) and Recital 81 GDPR.
[38] Recital 81 GDPR.
[39] Article 28(5) and Recital 81 GDPR.
[40] See also Article 28(3)h GDPR.
[41] Article 28(9) GDPR.

102. Furthermore, the contract or the other legal act under Union or Member State law must be **binding on the processor** with regard to the controller, i.e. it must establish obligations on the processor that are binding as a matter of EU or Member State law. Also it must set out the obligations of the controller. In most cases, there will be a contract, but the Regulation also refers to "other legal act", such as a national law (primary or secondary) or other legal instrument. If the legal act does not include all the minimum required content, it must be supplemented with a contract or another legal act that includes the missing elements.

103. Since the Regulation establishes a clear obligation to enter into a written contract, where no other relevant legal act is in force, the absence thereof is an infringement of the GDPR.[42] Both the controller and processor are responsible for ensuring that there is a contract or other legal act to govern the processing.[43] Subject to the provisions of Article 83 of the GDPR, the competent supervisory authority will be able to direct an administrative fine against both the controller and the processor, taking into account the circumstances of each individual case. Contracts that have been entered into before the date of application of the GDPR should have been updated in light of Article 28(3). The absence of such update, in order to bring a previously existing contract in line with the requirements of the GDPR, constitutes an infringement of Article 28(3).

A written contract pursuant to Article 28(3) GDPR may be embedded in a broader contract, such as a service level agreement. In order to facilitate the demonstration of compliance with the GDPR, the EDPB recommends that the elements of the contract that seek to give effect to Article 28 GDPR be clearly identified as such in one place (for example in an annex).

104. In order to comply with the duty to enter into a contract, **the controller and the processor may choose to negotiate their own contract** including all the compulsory elements **or to rely, in whole or in part, on standard contractual clauses in relation to obligations under Article 28**.[44]

[42] The presence (or absence) of a written arrangement, however, is not decisive for the existence of a controller-processor relationship. Where there is reason to believe that the contract does not correspond with reality in terms of actual control, on the basis of a factual analysis of the circumstances surrounding the relationship between the parties and the processing of personal data being carried out, the agreement may be set aside. Conversely, a controller-processor relationship might still be held to exist in absence of a written processing agreement. This would, however, imply a violation of Article 28(3) GDPR. Moreover, in certain circumstances, the absence of a clear definition of the relationship between the controller and the processor may raise the problem of the lack of legal basis on which every processing should be based, e.g. in respect of the communication of data between the controller and the alleged processor.
[43] Article 28(3) is not only applicable to controllers. In the situation where only the processor is subject to the territorial scope of the GDPR, the obligation shall only be directly applicable to the processor, see also EDPB Guidelines 3/2018 on the territorial scope of the GDPR, p. 12.
[44] Article 28(6) GDPR. The EDPB recalls that standard contractual clauses for the purposes of compliance with Article 28 GDPR are not the same as standard contractual clauses referred to in Article 46(2). While the former further stipulate and clarify how the provisions of Article 28(3) and (4) will be fulfilled, the latter provide appropriate safeguards in case of transfer of personal data to a third country or an international organisation in the absence of an adequacy decision pursuant to Article 45(3).

105. A set of standard contractual clauses (SCCs) may be, alternatively, adopted by the Commission[45] or adopted by a supervisory authority, in accordance with the consistency mechanism.[46] These clauses could be part of a certification granted to the controller or processor pursuant to Articles 42 or 43.[47]

106. The EDPB would like to clarify that there is no obligation for controllers and processors to enter into a contract based on SCCs, nor is it to be necessarily preferred over negotiating an individual contract. Both options are viable for the purposes of compliance with data protection law, depending on the specific circumstances, as long as they meet the Article 28(3) requirements.

107. If the parties wish to take advantage of standard contractual clauses, the data protection clauses of their agreement must be the same as those of the SCCs. The SCCs will often leave some blank spaces to be filled in or options to be selected by the parties. Also, as also mentioned above, the SCCs will generally be embedded in a larger agreement describing the object of the contract, its financial conditions, and other agreed clauses: it will be possible for the parties to add additional clauses (e.g. applicable law and jurisdiction) as long as they do not contradict, directly or indirectly, the SCCs[48] and they do not undermine the protection afforded by the GDPR and EU or Member State data protection laws.

108. Contracts between controllers and processors may sometimes be drafted unilaterally by one of the parties. Which party or parties that draft the contract may depend on several factors, including: the parties' position in the market and contractual power, their technical expertise, as well as access to legal services. For instance, some service providers tend to set up standard terms and conditions, which include data processing agreements.

109. An agreement between the controller and processor must comply with the requirements of Article 28 GDPR in order to ensure that the processor processes personal data in compliance with the GDPR. Any such agreement should take into account the specific responsibilities of controllers and processors. Although Article 28 provides a list of points which must be addressed in any contract governing the relationship between controllers and processors it leaves room for negotiations between the parties to such contracts. In some situations a controller or a processor may be in a weaker negotiation power to customize the data protection agreement. Reliance on the standard contractual clauses adopted pursuant to Article 28 (subparagraphs 7 and 8) may contribute to rebalancing the negotiating positions and to ensure that the contracts respect the GDPR.

[45] Article 28(7) GDPR. Article 28(7) GDPR. Article 28(7) GDPR. Article 28(7) GDPR. See the EDPB-EDPS Joint Opinion 1/2021 on standard contractual clauses between controllers and processors: https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-12021-standard_en.

[46] Article 28(8) GDPR. The Register for Decisions taken by supervisory authorities and courts on issues handled in the consistency mechanism, including standard contractual clauses for the purposes of compliance with Art. 28 GDPR, can be accessed here: https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-decisions_en.

[47] Article 28(6) GDPR.

[48] The EDPB recalls that the same degree of flexibility is allowed when the parties choose to use SCCs as appropriate safeguard for transfers to third countries pursuant to Article 46(2)(c) or Article 46(2)(d) GDPR. Recital 109 GDPR clarifies that "*The possibility for the controller or processor to use standard data-protection clauses adopted by the Commission or by a supervisory authority should prevent controllers or processors neither from including the standard data-protection clauses in a wider contract, such as a contract between the processor and another processor, nor from adding other clauses or additional safeguards provided that they do not contradict, directly or indirectly, the standard contractual clauses [...] or prejudice the fundamental rights or freedoms of the data subjects. Controllers and processors should be encouraged to provide additional safeguards via contractual commitments that supplement standard protection clauses*".

110. The fact that the contract and its detailed terms of business are prepared by the service provider rather than by the controller is not in itself problematic and is not in itself a sufficient basis to conclude that the service provider should be considered as a controller. Also, the imbalance in the contractual power of a small data controller with respect to big service providers should not be considered as a justification for the controller to accept clauses and terms of contracts which are not in compliance with data protection law, nor can it discharge the controller from its data protection obligations. The controller must evaluate the terms and in so far as it freely accepts them and makes use of the service, it has also accepted full responsibility for compliance with the GDPR. Any proposed modification, by a processor, of data processing agreements included in standard terms and conditions should be directly notified to and approved by the controller, bearing in mind the degree of leeway that the processor enjoys with respect to non-essential elements of the means (see paragraphs 40-41 above). The mere publication of these modifications on the processor's website is not compliant with Article 28.

1.3 Content of the contract or other legal act

111. Before focusing on each of the detailed requirements set out by the GDPR as to the content of the contract or other legal act, some general remarks are necessary.

112. While the elements laid down by Article 28 of the Regulation constitute its core content, the contract should be a way for the controller and the processor to further clarify how such core elements are going to be implemented with detailed instructions. Therefore, **the processing agreement should not merely restate the provisions of the GDPR**: rather, it should include more specific, concrete information as to how the requirements will be met and which level of security is required for the personal data processing that is the object of the processing agreement. Far from being a pro-forma exercise, the negotiation and stipulation of the contract are a chance to specify details regarding the processing.[49] Indeed, the "protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processors [...] requires a clear allocation of the responsibilities" under the GDPR.[50]

113. At the same time, the contract should **take into account "*the specific tasks and responsibilities of the processor in the context of the processing to be carried out and the risk to the rights and freedoms of the data subject*"**.[51] Generally speaking, the contract between the parties should be drafted in light of the specific data processing activity. For instance, there is no need to impose particularly stringent protections and procedures on a processor entrusted with a processing activity from which only minor risks arise: while each processor must comply with the requirements set out by the Regulation, the measures and procedures should be tailored to the specific situation. In any event, all elements of Article 28(3) must be covered by the contract. At the same time, the contract should include some elements that may help the processor in understanding the risks to the rights and freedoms of data subjects arising from the processing: because the activity is performed on behalf of the controller, often the controller has a deeper understanding of the risks that the processing entails since the controller is aware of the circumstances in which the processing is embedded.

114. Moving on to the **required content** of the contract or other legal act, EDPB interprets Article 28(3) in a way that it needs to set out:

[49] See also EDPB Opinion 14/2019 on the draft Standard Contractual Clauses submitted by the DK SA (Article 28(8) GDPR), p. 5.

[50] Recital 79 GDPR.

[51] Recital 81 GDPR.

- the **subject-matter** of the processing (for instance, video surveillance recordings of people entering and leaving a high-security facility). While the subject matter of the processing is a broad concept, it needs to be formulated with enough specifications so that it is clear what the main object of the processing is;
- the **duration**[52] of the processing: the exact period of time, or the criteria used to determine it, should be specified; for instance, reference could be made to the duration of the processing agreement;
- the **nature** of the processing: the type of operations performed as part of the processing (for instance: "filming", "recording", "archiving of images", ...) **and purpose** of the processing (for instance: detecting unlawful entry). This description should be as comprehensive as possible, depending on the specific processing activity, so as to allow external parties (e.g. supervisory authorities) to understand the content and the risks of the processing entrusted to the processor.
- the **type of personal data**: this should be specified in the most detailed manner as possible (for instance: video images of individuals as they enter and leave the facility). It would not be adequate merely to specify that it is "personal data pursuant to Article 4(1) GDPR" or "special categories of personal data pursuant to Article 9". In case of special categories of data, the contract or legal act should at least specify which types of data are concerned, for example, "information regarding health records", or "information as to whether the data subject is a member of a trade union";
- the **categories of data subjects**: this, too, should be indicated in a quite specific way (for instance: "visitors", "employees", delivery services etc.);
- the **obligations and rights of the controller**: the rights of the controller are further dealt with in the following sections (e.g. with respect to the right of the controller to perform inspections and audits). As regards the obligations of the controller, examples include the controller's obligation to provide the processor with the data mentioned in the contract, to provide and document any instruction bearing on the processing of data by the processor, to ensure, before and throughout the processing, compliance with the obligations set out in the GDPR on the processor's part, to supervise the processing, including by conducting audits and inspections with the processor.

115. While the GDPR lists elements that always need to be included in the agreement, other relevant information may need to be included, depending on the context and the risks of the processing as well as any additional applicable requirement.

1.3.1 The processor must only process data on documented instructions from the controller (Art. 28(3)(a) GDPR)

116. The need to specify this obligaton stems from the fact that the processor processes data on behalf of the controller. Controllers must provide its processors with instructions related to each processing activity. Such instructions can include permissible and unacceptable handling of personal data, more detailed procedures, ways of securing data, etc. The processor shall not go beyond what is instructed by the controller. It is however possible for the processor to suggest elements that, if accepted by the controller, become part of the instructions given.

[52] The duration of the processing is not necessarily equivalent to the duration of the agreement (there may be legal obligations to keep the data longer or shorter).

117. When a processor processes data outside or beyond the controller's instructions, and this amounts to a decision determining the purposes and means of processing, the processor will be in breach of its obligations and will even be considered a controller in respect of that processing in accordance with Article 28(10) (see sub-section 1.5 below[53]).

118. The instructions issued by the controller must be **documented**. For these purposes, it is recommended to include a procedure and a template for giving further instructions in an annex to the contract or other legal act. Alternatively, the instructions can be provided in any written form (e.g. e-mail), as well as in any other documented form as long as it is possible to keep records of such instructions. In any event, to avoid any difficulties in demonstrating that the controller's instructions have been duly documented, the EDPB recommends keeping such instructions together with the contract or other legal act.

119. The duty for the processor to refrain from any processing activity not based on the controller's instructions also applies to **transfers** of personal data to a third country or international organisation. The contract should specify the requirements for transfers to third countries or international organisations, taking into account the provisions of Chapter V of the GDPR.

120. The EDPB recommends that controller pay due attention to this specific point especially when the processor is going to delegate some processing activities to other processors, and when the processor has divisions or units located in third countries. If the instructions by the controller do not allow for transfers or disclosures to third countries, the processor will not be allowed to assign the processing to a sub-processor in a third country, nor will he be allowed to have the data processed in one of his non-EU divisions.

121. A processor may process data other than on documented instructions of the controller **when the processor is required to process and/or transfer personal data on the basis of EU law or Member State law to which the processor is subject**. This provision further reveals the importance of carefully negotiating and drafting data processing agreements, as, for example, legal advice may need to be sought by either party as to the existence of any such legal requirement. This needs to be done in a timely fashion, as the processor has an obligation to inform the controller of such requirement before starting the processing. Only when that same (EU or Member State) law forbids the processor to inform the controller on "important grounds of public interest", there is no such information obligation. In any case, any transfer or disclosure may only take place if authorised by Union law, including in accordance with Article 48 of the GDPR.

1.3.2 The processor must ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality (Art. 28(3)(b) GDPR)

122. The contract needs to state that the processor must ensure that anyone it allows to process the personal data is committed to confidentiality. This may occur either via a specific contractual agreement, or due to statutory obligations already in place.

123. The broad concept of "persons authorised to process the personal data" includes employees and temporary workers. Generally speaking, the processor should make the personal data available only to the employees who actually need them to perform tasks for which the processor was hired by the controller.

[53] See Part II, sub-section 1.5 ("Processor determining purposes and means of processing").

124. The commitment or obligation of confidentiality must be "appropriate", i.e. it must effectively forbid the authorised person from disclosing any confidential information without authorisation, and it must be sufficiently broad so as to encompass all the personal data processed on behalf of the controller as well as the conditions under which the personal data are processed.

1.3.3 The processor must take all the measures required pursuant to Article 32 (Art. 28(3)(c) GDPR)

125. Article 32 requires the controller and the processor to implement appropriate technical and organisational security measures. While this obligation is already directly imposed on the processor whose processing operations fall within the scope of the GDPR, the duty to take all measures required pursuant to Article 32 still needs to be reflected in the contract concerning the processing activities entrusted by the controller.

126. As indicated earlier, the processing contract should not merely restate the provisions of the GDPR. The contract needs to include or reference information as to the security measures to be adopted**, an obligation on the processor to obtain the controller's approval before making changes**, and a regular review of the security measures so as to ensure their appropriateness with regard to risks, which may evolve over time. The degree of detail of the information as to the security measures to be included in the contract must be such as to enable the controller to assess the appropriateness of the measures pursuant to Article 32(1) GDPR. Moreover, the description is also necessary in order to enable the controller to comply with its accountability duty pursuant to Article 5(2) and Article 24 GDPR as regards the security measures imposed on the processor. A corresponding obligation of the processor to assist the controller and to make available all information necessary to demonstrate compliance can be inferred from Art. 28.3 (f) and (h) GDPR.

127. The level of instructions provided by the controller to the processor as to the measures to be implemented will depend on the specific circumstances. In some cases, the controller may provide a clear and detailed description of the security measures to be implemented. In other cases, the controller may describe the minimum security objectives to be achieved, while requesting the processor to propose implementation of specific security measures. In any event, the controller must provide the processor with a description of the processing activities and security objectives (based on the controller's risk assessment), as well as approve the measures proposed by the processor. This could be included in an annex to the contract. The controller exercises its decision-making power over the main features of the security measures, be it by explicitly listing the measures or by approving those proposed by the processor.

1.3.4 The processor must respect the conditions referred to in Article 28(2) and 28(4) for engaging another processor (Art. 28(3)(d) GDPR).

128. The agreement must specify that the processor may not engage another processor without the controller's prior written authorisation and whether this authorisation will be specific or general. In case of general authorisation, the processor has to inform the controller of any change of sub-processors under a written authorisation, and give the controller the opportunity to object. It is recommended that the contract set out the process for this. It should be noted that the processor's duty to inform the controller of any change of sub-processors implies that the processor actively indicates or flags such changes toward the controller.[54] Also, where specific authorisation is required, the contract should set out the process for obtaining such authorisation.

129. When the processor engages another processor, a contract must be put in place between them, imposing the same data protection obligations as those imposed on the original processor or these obligations must be imposed by another legal act under Union or Member State law (see also below paragraph 160). This includes the obligation under Article 28(3)(h) to allow for and contribute to audits by the controller or another auditor mandated by the controller.[55] The processor is liable to the controller for the other processors' compliance with data protection obligations (for further details on the recommended content of the agreement see sub-section 1.6 below[56]).

1.3.5 The processor must assist the controller for the fulfilment of its obligation to respond to requests for exercising the data subject's rights (Article 28(3) (e) GDPR).

130. While ensuring that data subjects requests are dealt with is up to the controller, the contract must stipulate that the processor has an obligation to provide assistance "by appropriate technical and organisational measures, insofar as this is possible". The nature of this assistance may vary greatly "taking into account the nature of the processing" and depending on the type of activity entrusted to the processor. The details concerning the assistance to be provided by the processor should be included in the contract or in an annex thereto.

131. While the assistance may simply consist in promptly forwarding any request received and/or enabling the controller to directly extract and manage the relevant personal data, in some circumstances the processor will be given more specific, technical duties, especially when it is in the position of extracting and managing the personal data.

132. It is crucial to bear in mind that, although the practical management of individual requests can be outsourced to the processor, the controller bears the responsibility for complying with such requests. Therefore, the assessment as to whether requests by data subjects are admissible and/or the requirements set by the GDPR are met should be performed by the controller, either on a case-by-case basis or through clear instructions provided to the processor in the contract before the start of the processing. Also, the deadlines set out by Chapter III cannot be extended by the controller based on the fact that the necessary information must be provided by the processor.

1.3.6 The processor must assist the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 (Art. 28(3)(f) GDPR).

133. It is necessary for the contract to avoid merely restating these duties of assistance: **the agreement should contain details as to how the processor is asked to help the controller meet the listed obligations**. For example, procedures and template forms may be added in the annexes to the agreement, allowing the processor to provide the controller with all the necessary information.

134. The type and degree of assistance to be provided by the processor may vary widely "*taking into account the nature of processing and the information available to the processor*". The controller must

[54] In this regard it is, by contrast, e.g. not sufficient for the processor to merely provide the controller with a generalized access to a list of the sub-processors which might be updated from time to time, without pointing to each new sub-processor envisaged. In other words, the processor must actively inform the controller of any change to the list (i.e. in particular of each new envisaged sub-processor).
[55] See also EDPB Opinion 14/2019 on the draft Standard Contractual Clauses submitted by the DK SA (Article 28(8) GDPR), 9 July 2019, at paragraph 44.
[56] See Part II, sub-section 1.6 ("Sub-processors").

adequately inform the processor as to the risk involved in the processing and as to any other circumstance that may help the processor meet its duty.

135. Moving on to the specific obligations, the processor has, first, a duty to assist the controller in meeting the obligation to adopt adequate technical and organisational measures to ensure security of processing.[57] While this may overlap, to some extent, with the requirement that the processor itself adopts adequate security measures, where the processing operations of the processor fall within the scope of the GDPR, they remain two distinct obligations, since one refers to the processor's own measures and the other refers to the controller's.

136. Secondly, the processor must assist the controller in meeting the obligation to notify personal data breaches to the supervisory authority and to data subjects. The processor must notify the controller whenever it discovers a personal data breach affecting the processor's or a sub-processor's facilities / IT systems and help the controller in obtaining the information that need to be stated in the report to the supervisory authority.[58] The GDPR requires that the controller notify a breach without undue delay in order to minimize the harm for individuals and to maximize the possibility to address the breach in an adequate manner. Thus, the processor's notification to the data controller should also take place without undue delay.[59] Depending on the specific features of the processing entrusted to the processor, it may be appropriate for the parties to include in the contract a specific timeframe (e.g. number of hours) by which the processor should notify the controller, as well as the point of contact for such notifications, the modality and the minimum content expected by the controller.[60] The contractual arrangement between the controller and the processor may also include an authorisation and a requirement for the processor to directly notify a data breach in accordance with Articles 33 and 34, but the legal responsibility for the notification remains with the controller.[61] If the processor does notify a data breach directly to the supervisory authority, and inform data subjects in accordance with Article 33 and 34, the processor must also inform the controller and provide the controller with copies of the notification and information to data subjects.

137. Furthermore, the processor must also assist the controller in carrying out data protection impact assessments when required, and in consulting the supervisory authority when the outcome reveals that there is a high risk that cannot be mitigated.

138. The duty of assistance does not consist in a shift of responsibility, as those obligations are imposed on the controller. For instance, although the data protection impact assessment can in practice be carried out by a processor, the controller remains accountable for the duty to carry out the assessment[62] and the processor is only required to assist the controller "where necessary and upon request."[63] As a result, the controller is the one that must take the initiative to perform the data protection impact assessment, not the processor.

[57] Article 32 GDPR.
[58] Article 33(3) GDPR.
[59] For more information, see the Guidelines on Personal data breach notification under Regulation 2016/679, WP250rev.01, 6 February 2018, p. 13-14.
[60] See also EDPB Opinion 14/2019 on the draft Standard Contractual Clauses submitted by the DK SA (Article 28(8) GDPR), 9 July 2019, at paragraph 40.
[61] Guidelines on Personal data breach notification under Regulation 2016/679, WP250rev.01, 6 February 2018, p. 14.
[62] Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP 248 rev.01, p. 14
[63] Recital 95 GDPR.

1.3.7 On termination of the processing activities, the processor must, at the choice of the controller, delete or return all the personal data to the controller and delete existing copies (Art. 28(3)(g) GDPR).

139. The contractual terms are meant to ensure that the personal data are subject to appropriate protection after the end of the "provision of services related to the processing": it is therefore up to the controller to decide what the processor should do with regard to the personal data.

140. The controller can decide at the beginning whether personal data shall be deleted or returned by specifying it in the contract, through a written communication to be timely sent to the processor. The contract or other legal act should reflect the possibility for the data controller to change the choice made before the end of the provision of services related to the processing. The contract should specify the process for providing such instructions.

141. If the controller chooses that the personal data be deleted, the processor should ensure that the deletion is performed in a secure manner, also in order to comply with Article 32 GDPR. The processor should confirm to the controller that the deletion has been completed within an agreed timescale and in an agreed manner.

142. The processor must delete all existing copies of the data, unless EU or Member State law requires further storage. If the processor or controller is aware of any such legal requirement, it should inform the other party as soon as possible.

1.3.8 The processor must make available to the controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller (Art. 28(3)(h) GDPR).

143. The contract shall include details on how often and how the flow of information between the processor and the controller should take place so that the controller is fully informed as to the details of the processing that are relevant to demonstrate compliance with the obligations laid down in Article 28 GDPR. For instance, the relevant portions of the processor's records of processing activities may be shared with the controller. The processor should provide all information on how the processing activity will be carried out on behalf of the controller. Such information should include information on the functioning of the systems used, security measures, how the data retention requirements are met, data location, transfers of data, who has access to data and who are the recipients of data, sub-processors used, etc.

144. Further details shall also be set out in the contract regarding the ability to carry out and the duty to contribute to inspections and audits by the controller or another auditor mandated by the controller.

The GDPR specifies the inspections and audits are carried out by the controller or by a third party mandated by the controller. The goal of such audit is ensuring that the controller has all information concerning the processing activity performed on its behalf and the guarantees provided by the processor. The processor may suggest the choice of a specific auditor, but the final decision has to be left to the controller according to Article 28(3)(h) of the GDPR.[64] Additionally, even where the

[64] See EDPB-EDPS Joint Opinion 1/2021 on standard contractual clauses between controllers and processors, paragraph 43.

inspection is performed by an auditor proposed by the processor, the controller retains the right to contest the scope, methodology and results of the inspection.[65]

The parties should cooperate in good faith and assess whether and when there is a need to perform audits on the processor's premises,, as well as which type of audit or inspection (remote / on-site / other way to gather the necessary information) would be needed and appropriate in the specific case also taking into account security concerns; the final choice on this is to be taken by the controller. Following the results of the inspection, the controller should be able to request the processor to take subsequent measures, e.g. to remedy shortcomings and gaps identified.[66] Likewise, specific procedures should be established regarding the processor's and the controller's inspection of sub-processors (see sub-section 1.6 below[67]).

145. The issue of the allocation of costs between a controller and a processor concerning audits is not covered by the GDPR and is subject to commercial considerations. However, Article 28 (3)(h) requires that the contract include an obligation for the processor to make available all information necessary to the controller and an obligation to allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller. This means in practice that parties should not insert in the contract clauses envisaging the payment of costs or fees that would be clearly disproportionate or excessive, thus having a dissuasive effect on one of the parties. Such clauses would indeed imply that the rights and obligations set out in Article 28(3)(h) would never be exercised in practice and would become purely theoretical whereas they form an integral part of the data protection safeguards envisaged under Article 28 GDPR.

1.4 Instructions infringing data protection law

146. According to Article 28(3), the processor must immediately inform the controller if, in its opinion, an instruction infringes the GDPR or other Union or Member State data protection provisions.

147. Indeed, the processor has a duty to comply with the controller's instructions, but it also has a general obligation to comply with the law. An instruction that infringes data protection law seems to cause a conflict between the aforementioned two obligations.

148. Once informed that one of its instructions may be in breach of data protection law, the controller will have to assess the situation and determine whether the instruction actually violates data protection law.

149. The EDPB recommends the parties to negotiate and agree in the contract the consequences of the notification of an infringing instruction sent by the processor and in case of inaction from the controller in this context. One example would be to insert a clause on the termination of the contract if the controller persists with an unlawful instruction. Another example would be a clause on the possibility for the processor to suspend the implementation of the affected instruction until the controller confirms, amends or withdraws its instruction[68].

[65] See Opinion 14/2019 on the draft Standard Contractual Clauses submitted by the DK SA (Article 28(8) GDPR), paragraph 43.
[66] See Opinion 14/2019 on the draft Standard Contractual Clauses submitted by the DK SA (Article 28(8) GDPR), paragraph 43.
[67] See Part II, sub-section 1.6 ("Sub-processors").
[68] See EDPB-EDPS Joint Opinion 1/2021 on standard contractual clauses between controllers and processors, paragraph 39.

1.5 Processor determining purposes and means of processing

150. If the processor infringes the Regulation by determining the purposes and means of processing, it shall be considered as a controller in respect of that processing (Article 28(10) GDPR).

1.6 Sub-processors

151. Data processing activities are often carried out by a great number of actors, and the chains of subcontracting are becoming increasingly complex. The GDPR introduces specific obligations that are triggered when a (sub-)processor intends to engage another player, thereby adding another link to the chain, by entrusting to it activities requiring the processing of personal data. The analysis of whether the service provider acts as a sub-processor should be carried out in line with what described above on the concept of processor (see above paragraph 83).

152. Although the chain may be quite long, the controller retains its pivotal role in determining the purpose and means of processing. Article 28(2) GDPR stipulates that the processor shall not engage another processor without prior specific or general written authorisation of the controller (including in electronic form). In the case of general written authorisation, the processor must inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes. In both cases, the processor must obtain the controller's authorisation in writing before any personal data processing is entrusted to the sub-processor. In order to make the assessment and the decision whether to authorise subcontracting, a list of intended sub-processors (including per each: their locations, what they will be doing and proof of what safeguards have been implemented) will have to be provided to the data controller by the processor.[69]

153. The prior written authorisation may be specific, i.e. referring to a specific sub-processor for a specific processing activity and at a specific time, or general. This should be specified in the contract or other legal act that governs the processing.

154. In cases where the controller decides to accept certain sub-processors at the time of the signature of the contract, a list of approved sub-processors should be included in the contract or an annex thereto. The list should then be kept up to date, in accordance with the general or specific authorisation given by the controller.

155. If the controller chooses to give its **specific authorisation**, it should specify in writing which sub-processor and what processing activity it refers to. Any subsequent change will need to be further authorised by the controller before it is put in place. If the processor's request for a specific authorisation is not answered to within the set timeframe, it should be held as denied. The controller should make its decision to grant or withhold authorisation taking into account its obligation to only use processors providing "sufficient guarantees" (see sub-section 1.1 above[70]).

156. Alternatively, the controller may provide its **general authorisation** to the use of sub-processors (in the contract, including a list with such sub-processors in an annex thereto), which should be supplemented with criteria to guide the processor's choice (e.g., guarantees in terms of technical and organisational

[69] This information is needed, so that the controller can comply with the accountability principle in Article 24 and with provisions of Articles 28(1), 32 and Chapter V of the GDPR.
[70] See Part II - sub-section 1.1 ("Choice of the processor").

measures, expert knowledge, reliability and resources).[71] In this scenario, the processor needs to inform the controller in due time of any intended addition or replacement of sub-processor(s) so as to provide the controller with the opportunity to object.

157. Therefore, the main difference between the specific authorisation and the general authorisation scenarios lies in the meaning given to the controller's silence: in the general authorisation situation, the controller's failure to object within the set timeframe can be interpreted as authorisation.

158. In both scenarios, the contract should include details as to the timeframe for the controller's approval or objection and as to how the parties intend to communicate regarding this topic (e.g. templates). Such timeframe needs to be reasonable in light of the type of processing, the complexity of the activities entrusted to the processor (and the sub-processors) and the relationship between the parties. In addition, the contract should include details as to the practical steps following the controller's objection (e.g. by specifying time frame within which the controller and processor should decide whether the processing shall be terminated).

159. Regardless of the criteria suggested by the controller to choose providers, the processor remains fully liable to the controller for the performance of the sub-processors' obligations (Article 28(4) GDPR). Therefore, the processor should ensure it proposes sub-processors providing sufficient guarantees.

160. Furthermore, when a processor intends to employ an (authorised) sub-processor, it must enter into a contract with it that imposes the same obligations as those imposed on the first processor by the controller or the obligations must be imposed by another legal act under EU or Member State law. The whole chain of processing activities needs to be regulated by written agreements. Imposing the "same" obligations should be construed in a functional rather than in a formal way: it is not necessary for the contract to include exactly the same words as those used in the contract between the controller and the processor, but it should ensure that the obligations in substance are the same. This also means that if the processor entrusts the sub-processor with a specific part of the processing, to which some of the obligations cannot apply, such obligations should not be included "by default" in the contract with the sub-processor, as this would only generate uncertainty. As an example, as to assistance with data breach related obligations, notification of a data breach by a sub-processor directly to the controller could be done if all three agree. However, in the case of such direct notification the processor should be informed and get a copy of the notification.

2 CONSEQUENCES OF JOINT CONTROLLERSHIP

2.1 Determining in a transparent manner the respective responsibilities of joint controllers for compliance with the obligations under the GDPR

161. Article 26(1) of the GDPR provides that joint controllers shall in a transparent manner determine and agree on their respective responsibilities for compliance with the obligations under the Regulation.

162. Joint controllers thus need to set "who does what" by deciding between themselves who will have to carry out which tasks in order to make sure that the processing complies with the applicable obligations under the GDPR in relation to the joint processing at stake. In other words, a distribution of responsibilities for compliance is to be made as resulting from the use of the term "*respective*" in

[71] This duty of the controller stems from the accountability principle in Article 24 and from the obligation to comply with provisions of Articles 28(1), 32 and Chapter V of the GDPR.

Article 26(1). This does not preclude the fact that EU or Member State law may already set out certain responsibilities of each joint controller. Where this is the case, the joint controller arrangement should also address any additional responsibilities necessary to ensure compliance with the GDPR that are not addressed by the legal provisions.[72]

163. The objective of these rules is to ensure that where multiple actors are involved, especially in complex data processing environments, responsibility for compliance with data protection rules is clearly allocated in order to avoid that the protection of personal data is reduced, or that a negative conflict of competence lead to loopholes whereby some obligations are not complied with by any of the parties involved in the processing. It should be made clear here that all responsibilities have to be allocated according to the factual circumstances in order to achieve an operative agreement. The EDPB observes that there are situations occurring in which the influence of one joint controller and its factual influence complicate the achievement of an agreement. However, those circumstances do not negate the joint controllership and cannot serve to exempt either party from its obligations under the GDPR.

164. More specifically, Article 26(1) specifies that the determination of their respective responsibilities (i.e. tasks) for compliance with the obligations under the GDPR is to be carried out by joint controllers "*in particular*" as regards the exercising of the rights of the data subject and the duties to provide information referred in Articles 13 and 14, unless and in so far as the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject.

165. It is clear from this provision that joint controllers need to define who respectively will be in charge of answering to requests when data subjects exercise their rights granted by the GDPR and of providing information to them as required by Articles 13 and 14 of the GDPR. This only refers to defining in their internal relationship which of the parties is obligated to respond to which data subjects' requests. . Regardless of any such arrangement, the data subject may contact either of the joint controllers in accordance with Article 26 (3) GPDR. However, the use of the terms "*in particular*" indicates that the obligations subject to the allocation of responsibilities for compliance by each party involved as referred in this provision are non-exhaustive. It follows that the distribution of the responsibilities for compliance among joint controllers is not limited to the topics referred in Article 26(1) but extends to other controller's obligations under the GDPR. Indeed, joint controllers need to ensure that the whole joint processing fully complies with the GDPR.

166. In this perspective, the compliance measures and related obligations joint controllers should consider when determining their respective responsibilities, in addition to those specifically referred in Article 26(1), include amongst others without limitation:

- Implementation of general data protection principles (Article 5)
- Legal basis of the processing[73] (Article 6)
- Security measures (Article 32)

[72] "In any event, the joint controller arrangement should comprehensively address all of the responsibilities of the joint controllers, including those which may have already been set out in the relevant EU or Member State law and without prejudice to the obligation of joint controllers to make available the essence of the joint controller arrangement in accordance with Article 26(2) GDPR."

[73] Although the GDPR does not preclude joint controllers to use different legal basis for different processing operations they carry out, it is recommended to use, whenever possible, the same legal basis for a particular purpose.

- Notification of a personal data breach to the supervisory authority and to the data subject[74] (Articles 33 and 34)
- Data Protection Impact Assessments (Articles 35 and 36)[75]
- The use of a processor (Article 28)
- Transfers of data to third countries (Chapter V)
- Organisation of contact with data subjects and supervisory authorities

167. Other topics that could be considered depending on the processing at stake and the intention of the parties are for instance the limitations on the use of personal data for another purpose by one of the joint controllers. In this respect, both controllers always have a duty to ensure that they both have a legal basis for the processing. Sometimes, in the context of joint controllership, personal data are shared by one controller to another. As a matter of accountability, each controller has the duty to ensure that the data are not further processed in a manner that is incompatible with the purposes for which they were originally collected by the controller sharing the data.[76]

168. Joint controllers can have a certain degree of flexibility in distributing and allocating obligations among them as long as they ensure full compliance with the GDPR with respect of the given processing. The allocation should take into account factors such as, who is competent and in a position to effectively ensure data subject's rights as well as to comply with the relevant obligations under the GDPR. The EDPB recommends documenting the relevant factors and the internal analysis carried out in order to allocate the different obligations. This analysis is part of the documentation under the accountability principle.

169. The obligations do not need to be equally distributed among the joint controllers. In this respect, the CJEU has recently stated that "*the existence of joint responsibility does not necessarily imply equal responsibility of the various operators involved in the processing of personal data*".[77] However, there may be cases where not all of the obligations can be distributed and all joint controllers may need to comply with the same requirements arising from the GDPR, taking into account the nature and context of the joint processing. For instance, joint controllers using shared data processing tools or systems both need to ensure compliance with notably the purpose limitation principle and implement appropriate measures to ensure the security of personal data processed under the shared tools.

[74] Please also see EDPB guidelines on Personal data breach notification under Regulation 2016/679, WP250.rev.01 which provide that joint controllership will include "*determining which party will have responsibility for complying with the obligations under Articles 33 and 34. WP29 recommends that the contractual arrangements between joint controllers include provisions that determine which controller will take the lead on, or be responsible for, compliance with the GDPR's breach notification obligations*"(p.13).

[75] Please also see EDPB guidelines on DPIAs, WP248.rev01 which provide the following: "*When the processing operation involves joint controllers, they need to define their respective obligations precisely. Their DPIA should set out which party is responsible for the various measures designed to treat risks and to protect the rights and freedoms of the data subjects. Each data controller should express his needs and share useful information without either compromising secrets (e.g.: protection of trade secrets, intellectual property, confidential business information) or disclosing vulnerabilities*" (p.7).

[76] Each disclosure by a controller requires a lawful basis and assessment of compatibility, regardless of whether the recipient is a separate controller or a joint controller. In other words, the existence of a joint controller relationship does not automatically mean that the joint controller receiving the data can also lawfully process the data for additional purposes which are beyond the scope of joint control.

[77] Judgment in *Wirtschaftsakademie*, C-210/16, ECLI:EU:C:2018:388, paragraph 43.

170. Another example is the requirement for each joint controller to maintain a record of processing activities or to designate a Data Protection Officer (DPO) if the conditions of Article 37(1) are met. Such requirements are not related to the joint processing but are applicable to them as controllers.

2.2 Allocation of responsibilities needs to be done by way of an arrangement

2.2.1 Form of the arrangement

171. Article 26(1) of the GDPR provides as a new obligation for joint controllers that they should determine their respective responsibilities "*by means of an arrangement between them*". The legal form of such arrangement is not specified by the GDPR. Therefore, joint controllers are free to agree on the form of the arrangement.

172. In addition, the arrangement on the allocation of responsibilities is binding upon each of the joint controllers. They each agree and commit *vis-à-vis* each other on being responsible for complying with the respective obligations stated in their arrangement as their responsibility.

173. Therefore, for the sake of legal certainty, even if there is no legal requirement in the GDPR for a contract or other legal act, the EDPB recommends that such arrangement be made in the form of a binding document such as a contract or other legal binding act under EU or Member State law to which the controllers are subject. This would provide certainty and could be used to evidence transparency and accountability. Indeed, in case of non-compliance with the agreed allocation provided in the arrangement, its binding nature allows one controller to seek the liability of the other for what was stated in the agreement as falling under its responsibility. Also, in line with the accountability principle, the use of a contract or other legal act will allow joint controllers to demonstrate that they comply with the obligations imposed upon them by the GDPR.

174. The way responsibilities, i.e. the tasks, are allocated between each joint controller has to be stated in a clear and plain language in the arrangement.[78] This requirement is important as it ensures legal certainty and avoid possible conflicts not only in the relation between the joint controllers but also vis-à-vis the data subjects and the data protection authorities.

175. To better frame the allocation of responsibilities between the parties, the EDPB recommends that the arrangement also provide general information on the joint processing by notably specifying the subject matter and purpose of the processing, the type of personal data, and the categories of data subjects.

2.2.2 Obligations towards data subjects

176. The GDPR provides several obligations of joint controllers towards data subjects:

The arrangement shall duly reflect the respective roles and relationships of the joint controllers *vis-à-vis* the data subjects

177. As a complement to what is explained above in section 2.1 of the present guidelines, it is important that the joint controllers clarify in the arrangement their respective role, "*in particular*" as regards the exercise of the rights of the data subject and their duties to provide the information referred to in Articles 13 and 14. Article 26 of the GDPR stresses the importance of these specific obligations. The joint controllers must therefore organise and agree on how and by whom the information will be

[78] As stated in Recital 79 of the GDPR *"(...) the responsibility and liability of controllers and processors, also in relation to the monitoring by and measures of supervisory authorities, requires a clear allocation of the responsibilities under this Regulation, including where a controller determines the purposes and means of the processing jointly with other controllers*".

provided and how and by whom the answers to the data subject's requests will be provided. Irrespective of the content of the arrangement on this specific point, the data subject may contact either of the joint controllers to exercise his or her rights in accordance with Article 26(3) as further explained below.

178. The way these obligations are organised in the arrangement should "*duly*", i.e. accurately, reflect the reality of the underlying joint processing. For example, if only one of the joint controllers communicates with the data subjects for the purpose of the joint processing, such controller could be in a better position to inform the data subjects and possibly to answer their requests.

The essence of the arrangement shall be made available to the data subject

179. This provision is aimed to ensure that the data subject is aware of the "*essence of the arrangement*". For example, it must be completely clear to a data subject which data controller serves as a point of contact for the exercise of data subject rights (notwithstanding the fact that he or she can exercise his or her rights in respect of and against each joint controller). The obligation to make the essence of the arrangement available to data subjects is important in case of joint controllership in order for the data subject to know which of the controllers is responsible for what.

180. What should be covered by the notion of "*essence of the arrangement*" is not specified by the GDPR. The EDPB recommends that the essence cover at least all the elements of the information referred to in Articles 13 and 14 that should already be accessible to the data subject, and for each of these elements, the arrangement should specify which joint controller is responsible for ensuring compliance with these elements. The essence of the arrangement must also indicate the contact point, if designated.

181. The way such information shall be made available to the data subject is not specified. Contrary to other provisions of the GDPR (such as Article 30(4) for the record of processing or Article 40(11) for the register of approved codes of conduct), Article 26 does not indicate that the availability should be "*upon request*" nor "*publicly available by way of appropriate means*". Therefore, it is up to the joint controllers to decide the most effective way to make the essence of the arrangement available to the data subjects (e.g. together with the information in Article 13 or 14, in the privacy policy or upon request to the data protection officer, if any, or to the contact point that may have been designated). Joint controllers should respectively ensure that the information is provided in a consistent manner.

The arrangement may designate a contact point for data subjects

182. Article 26(1) provides the possibility for joint controllers to designate in the arrangement a contact point for data subjects. Such designation is not mandatory.

183. Being informed of a single way to contact possible multiple joint controllers enables data subjects to know who they can contact with regard to all issues related to the processing of their personal data. In addition, it allows multiple joint controllers to coordinate in a more efficient manner their relations and communications *vis-à-vis* data subjects.

184. For these reasons, in order to facilitate the exercise of data subjects' rights under the GDPR, the EDPB recommends joint controllers to designate such contact point.

185. The contact point can be the DPO, if any, the representative in the Union (for joint controllers not established in the Union) or any other contact point where information can be obtained.

Irrespective of the terms of the arrangement, data subjects may exercise their rights in respect of and against each of the joint controllers.

186. Under Article 26(3), a data subject is not bound by the terms of the arrangement and may exercise his or her rights under the GDPR in respect of and against each of the joint data controllers.

187. For example, in case of joint controllers established in different Member States, or if only one of the joint controllers is established in the Union, the data subject may contact, at his or her choice, either the controller established in the Member State of his or her habitual residence or place of work, or the controller established elsewhere in the EU or in the EEA.

188. Even if the arrangement and the available essence of it indicate a contact point to receive and handle all data subjects' requests, the data subjects themselves may still choose otherwise.

189. Therefore, it is important that joint controllers organise in advance in their arrangement how they will manage answers to requests they could receive from data subjects. In this respect, it is recommended that joint controllers communicate to the other controllers in charge or to the designated contact point, the requests received in order to be effectively handled. Requiring data subjects to contact the designated contact point or the controller in charge would impose an excessive burden on the data subject that would be contrary to the objective of facilitating the exercise of their rights under the GDPR.

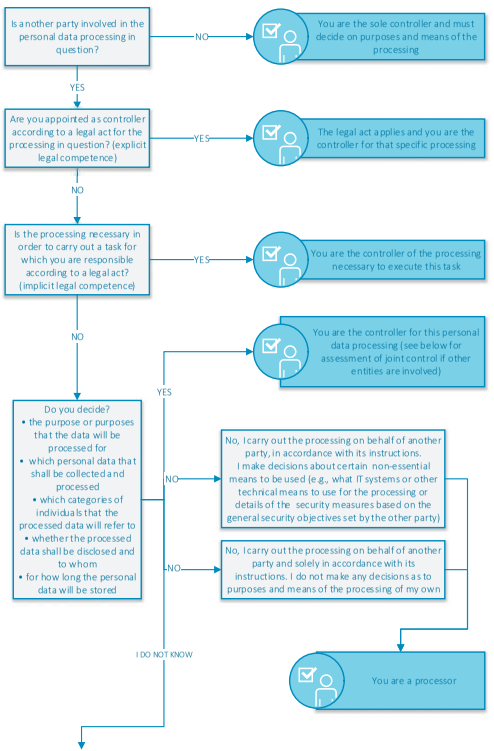
2.3 Obligations towards data protection authorities

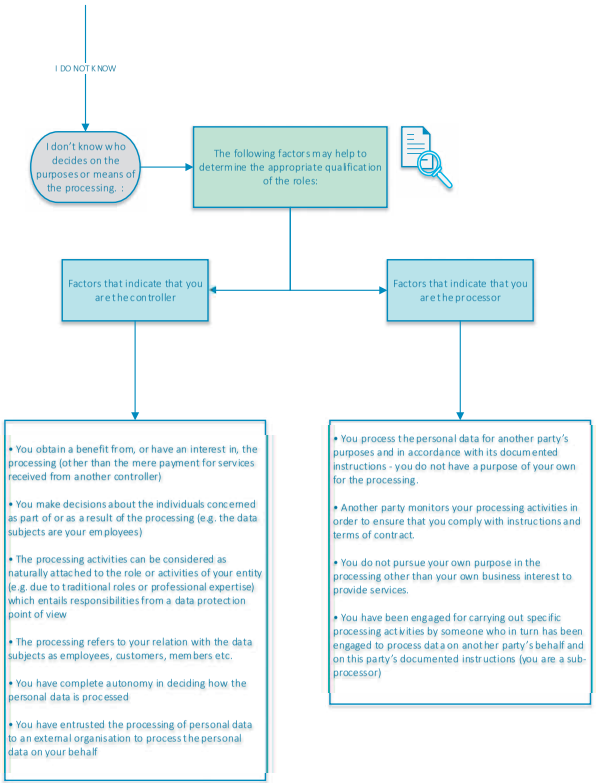
190. Joint controllers should organise in the arrangement the way they will communicate with the competent supervisory data protection authorities. Such communication could cover possible consultation under Article 36 of the GDPR, notification of a personal data breach, designation of a data protection officer.

191. It should be recalled that data protection authorities are not bound by the terms of the arrangement whether on the issue of the qualification of the parties as joint controllers or the designated contact point. Therefore, the authorities can contact any of the joint controllers to exercise their powers under Article 58 with respect to the joint processing.

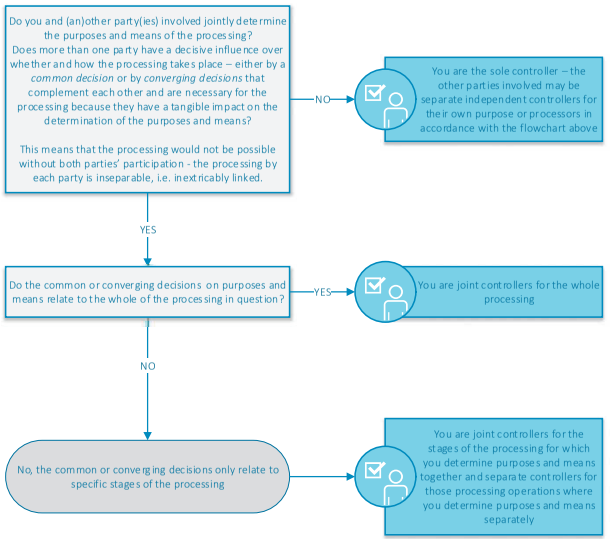
Annex I – Flowchart for applying the concepts of controller, processor and joint controllers in practice

Note: in order to properly assess the role of each entity involved, one must first identify the specific personal data processing at stake and its exact purpose. If multiple entities are involved, it is necessary to assess whether the purposes and means are determined jointly, leading to joint controllership.





Joint controllership - If you are the controller and other parties are involved in the personal data processing:





Wytyczne 6/2020 w sprawie wzajemnych zależności między dyrektywą PSD2 a RODO

Wersja 2.0

przyjęte 15 grudnia 2020 r.

Historia wersji

Wersja 2.0	15.12.2020 r.	Przyjęcie wytycznych po konsultacjach publicznych
Wersja 1.0	17.07.2020 r.	Przyjęcie wytycznych do konsultacji w sprawie publikacji

Spis treści

1. Wprowadzenie 5
1.1 Definicje 6
1.2 Usługi, o których mowa w PSD2 7
2 Zgodne z prawem podstawy i dalsze przetwarzanie na podstawie PSD2 10
2.1 Zgodne z prawem podstawy przetwarzania 10
2.2 Art. 6 ust. 1 lit. b RODO (przetwarzanie jest niezbędne do wykonania umowy) 10
2.3 Zapobieganie nadużyciom 12
2.4 Dalsze przetwarzanie (dostawcy świadczący usługę dostępu do informacji o rachunku i dostawcy świadczący usługę inicjowania płatności) 12
2.5 Zgodna z prawem podstawa udzielenia dostępu do rachunku (dostawcy usług płatniczych prowadzący rachunek) 13
3 Wyraźna zgoda 15
3.1 Zgoda w rozumieniu RODO 15
3.2 Zgoda w rozumieniu PSD2 15
3.2.1 Wyraźna zgoda w rozumieniu art. 94 ust. 2 PSD2 16
3.3 Podsumowanie 17
4 Przetwarzanie danych milczącej strony 19
4.1 Dane milczącej strony 19
4.2 Prawnie uzasadniony interes administratora 19
4.3 Dalsze przetwarzanie danych osobowych milczącej strony 19
5 Przetwarzanie szczególnych kategorii danych osobowych na podstawie PSD2 21
5.1 Szczególne kategorie danych osobowych 21
5.2 Możliwe wyjątki 22
5.3 Ważny interes publiczny 22
5.4 Wyraźna zgoda 22
5.5 Brak odpowiedniego wyjątku 23
6 Minimalizacja danych, bezpieczeństwo, przejrzystość, rozliczalność i profilowanie 24
6.1 Minimalizacja danych i uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych 24
6.2 Środki minimalizacji danych 24
6.3 Bezpieczeństwo 26
6.4 Przejrzystość i rozliczalność 26
6.5 Profilowanie 28

Europejska Rada Ochrony Danych

uwzględniając art. 70 ust. 1 lit. e) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (zwanego dalej „RODO"),

uwzględniając Porozumienie EOG, w szczególności załącznik XI i protokół 37 do tego Porozumienia, zmienione decyzją Wspólnego Komitetu EOG nr 154/2018 z dnia 6 lipca 2018 r.[1],

uwzględniając art. 12 i 22 swojego regulaminu wewnętrznego,

a także mając na uwadze, co następuje:

(1) Ogólne rozporządzenie o ochronie danych przewiduje spójny zestaw przepisów dotyczących przetwarzania danych osobowych w całej UE.

(2) Drugą dyrektywą w sprawie usług płatniczych (dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r., zwana dalej „PSD2") uchylono dyrektywę 2007/64/WE i ustanowiono nowe przepisy mające na celu zapewnienie pewności prawa konsumentom, akceptantom i przedsiębiorstwom w łańcuchu płatności oraz modernizację ram prawnych dla rynku usług płatniczych[2]. Państwa członkowskie miały dokonać transpozycji PSD2 do prawa krajowego przed dniem 13 stycznia 2018 r.

(3) Ważną cechą PSD2 jest wprowadzenie ram prawnych dla nowych usług inicjowania płatności i usług dostępu do informacji o rachunku. PSD2 umożliwia dostawcom tych nowych usług płatniczych uzyskanie dostępu do rachunków płatniczych osób, których dane dotyczą, w celu świadczenia wspomnianych usług.

(4) Jeżeli chodzi o ochronę danych, zgodnie z art. 94 ust. 1 PSD2 wszelkie przetwarzanie danych osobowych, w tym przekazywanie informacji o przetwarzaniu, na potrzeby PSD2 odbywa się zgodnie z RODO[3] oraz z rozporządzeniem (UE) 2018/1725.

(5) Motyw 89 PSD2 stanowi, że w przypadku przetwarzania danych osobowych do celów PSD2 należy określić dokładny cel, przywołać stosowną podstawę prawną, spełnić stosowne wymogi dotyczące bezpieczeństwa ustanowione w RODO, a także przestrzegać zasad konieczności, proporcjonalności, ograniczenia celu oraz proporcjonalnego okresu zatrzymywania danych. Ponadto uwzględnienie ochrony danych już w fazie projektowania i domyślna ochrona danych powinny być wbudowane we wszystkie systemy przetwarzania danych opracowywane i używane w ramach PSD2[4].

(6) Motyw 93 PSD2 stanowi, że dostawcy świadczący usługę inicjowania płatności i dostawcy świadczący usługę dostępu do informacji o rachunku, z jednej strony, oraz dostawca usług płatniczych prowadzący rachunek, z drugiej strony, powinni przestrzegać niezbędnych wymogów w zakresie ochrony danych i bezpieczeństwa, które zostały określone lub o których mowa w niniejszej dyrektywie lub które uwzględniono w regulacyjnych standardach technicznych.

PRZYJĘŁA NASTĘPUJĄCE WYTYCZNE:

1. WPROWADZENIE

1. Druga dyrektywa w sprawie usług płatniczych (dalej jako: „PSD2") wprowadziła szereg nowości w obszarze usług płatniczych. Chociaż stwarza ona nowe możliwości dla konsumentów i zwiększa przejrzystość w tym obszarze, stosowanie PSD2 rodzi pewne pytania i obawy związane z koniecznością zachowania przez osoby, których dane dotyczą, pełnej kontroli nad własnymi danymi osobowymi. Ogólne rozporządzenie o ochronie danych (zwane dalej „RODO") ma zastosowanie do przetwarzania danych osobowych, w tym do czynności przetwarzania dokonywanych w kontekście usług płatniczych, określonych w PSD2[5]. W związku z tym administratorzy działający w obszarze objętym PSD2 muszą zawsze zapewniać zgodność z wymogami RODO, w tym z zasadami ochrony danych określonymi w art. 5 RODO, jak również z odpowiednimi przepisami dyrektywy o prywatności i łączności elektronicznej[6]. Chociaż PSD2[7] oraz regulacyjne standardy techniczne dotyczące silnego uwierzytelniania klienta oraz wspólnych i bezpiecznych otwartych standardów komunikacji (zwane dalej „regulacyjnymi standardami technicznymi"[8]) zawierają określone przepisy dotyczące ochrony i bezpieczeństwa danych, pojawiła się niepewność co do interpretacji tych przepisów, jak również wzajemnych zależności między ogólnymi ramami ochrony danych a PSD2.
2. 5 lipca 2018 r. EROD wydała pismo dotyczące PSD2, w którym udzieliła wyjaśnień w kwestiach dotyczących ochrony danych osobowych w związku z tą dyrektywą, w szczególności w zakresie przetwarzania danych osobowych nieumawiających się stron (tzw. danych milczącej strony) przez dostawców świadczących usługę dostępu do informacji o rachunku oraz dostawców świadczących usługę inicjowania płatności, procedur dotyczących wyrażania i wycofywania zgody, regulacyjnych standardów technicznych oraz współpracy pomiędzy dostawcami usług płatniczych prowadzącymi rachunek w odniesieniu do środków bezpieczeństwa. Z kolei prace przygotowawcze nad niniejszymi wytycznymi obejmowały zebranie uwag od zainteresowanych stron, zarówno w formie pisemnej, jak i podczas spotkania z zainteresowanymi stronami, w celu określenia najpilniejszych wyzwań.
3. Niniejsze wytyczne służą zapewnieniu dalszych wskazówek dotyczących aspektów ochrony danych w kontekście PSD2, w szczególności powiązań między odpowiednimi przepisami RODO i PSD2. Największy nacisk w wytycznych położono na przetwarzanie danych osobowych przez dostawców

[1] Odniesienia do „państw członkowskich" zawarte w niniejszym dokumencie należy rozumieć jako odniesienia do „państw członkowskich EOG".
[2] Motyw 6 PSD2.
[3] W związku z tym, że PSD2 powstała przed RODO, nadal zawiera odniesienia do dyrektywy 95/46/WE. Art. 94 RODO stanowi, że odesłania do uchylonej dyrektywy 95/46/EW należy traktować jako odesłania do RODO.
[4] Motyw 89 PSD2.
[5] Art. 1 ust. 1 RODO.
[6] Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej); Dz.U. L 201 z 31.7.2002, s. 37.
[7] Art. 94 PSD2 itp.
[8] Rozporządzenie delegowane Komisji (UE) 2018/389 z dnia 27 listopada 2017 r. uzupełniające dyrektywę Parlamentu Europejskiego i Rady (UE) 2015/2366 w odniesieniu do regulacyjnych standardów technicznych dotyczących silnego uwierzytelniania klienta i wspólnych i bezpiecznych otwartych standardów komunikacji (Tekst mający znaczenie dla EOG.); C/2017/7782; Dz.U. L 69 z 13.3.2018, s. 23-43; dostępne pod adresem https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32018R0389&from=EN

świadczących usługę dostępu do informacji o rachunku oraz dostawców świadczących usługę inicjowania płatności. W związku z tym niniejszy dokument dotyczy warunków udzielania dostępu do informacji o rachunku płatniczym przez dostawców usług płatniczych prowadzących rachunek oraz przetwarzania danych osobowych przez dostawców świadczących usługę inicjowania płatności i dostawców świadczących usługę dostępu do informacji o rachunku, w tym wymogów i środków ochronnych w odniesieniu do przetwarzania danych osobowych przez dostawców świadczących usługę inicjowania płatności i dostawców świadczących usługę dostępu do informacji o rachunku w celach innych niż pierwotne cele, dla których zgromadzono dane, w szczególności gdy zgromadzono je w kontekście świadczenia usługi dostępu do informacji o rachunku[9]. W niniejszym dokumencie odniesiono się również do odmiennych pojęć wyraźnej zgody na podstawie PSD2 i RODO, przetwarzania „danych milczącej strony", przetwarzania szczególnych kategorii danych osobowych przez dostawców świadczących usługę inicjowania płatności i dostawców świadczących usługę dostępu do informacji o rachunku, stosowania głównych zasad ochrony danych określonych w RODO, w tym minimalizacji danych, przejrzystości, rozliczalności i środków bezpieczeństwa. PSD2 obejmuje wielofunkcyjne obowiązki m.in. w obszarze ochrony konsumentów i prawa konkurencji. Rozważania dotyczące wspomnianych dziedzin prawa wykraczają poza zakres niniejszych wytycznych.

4. Aby ułatwić lekturę wytycznych, poniżej podano główne definicje stosowane w niniejszym dokumencie.

1.1 Definicje

„Dostawca świadczący usługę dostępu do informacji o rachunku" oznacza dostawcę usługi online polegającej na dostarczaniu skonsolidowanych informacji na temat co najmniej jednego rachunku płatniczego posiadanego przez danego użytkownika usług płatniczych u innego dostawcy usług płatniczych albo u więcej niż jednego dostawcy usług płatniczych;

„dostawca usług płatniczych prowadzący rachunek" oznacza dostawcę usług płatniczych zapewniającego i utrzymującego rachunek płatniczy dla płatnika;

„minimalizacja danych" jest zasadą ochrony danych, zgodnie z którą dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane;

„płatnik" oznacza osobę fizyczną lub prawną, która jest posiadaczem rachunku płatniczego i zezwala na wykonanie zlecenia płatniczego z tego rachunku płatniczego, lub w przypadku gdy rachunek płatniczy nie istnieje – osobę fizyczną lub prawną, która składa zlecenie płatnicze;

„odbiorca" oznacza osobę fizyczną lub prawną będącą zamierzonym odbiorcą środków pieniężnych, które są przedmiotem transakcji płatniczej;

„rachunek płatniczy" oznacza rachunek prowadzony w imieniu co najmniej jednego użytkownika usług płatniczych, wykorzystywany do wykonywania transakcji płatniczych;

„dostawca świadczący usługę inicjowania płatności" oznacza dostawcę świadczącego usługę polegającą na zainicjowaniu zlecenia płatniczego na wniosek użytkownika usług płatniczych w odniesieniu do rachunku płatniczego posiadanego u innego dostawcy usług płatniczych;

[9] Usługa dostępu do informacji o rachunku to usługa online polegająca na dostarczaniu skonsolidowanych informacji na temat co najmniej jednego rachunku płatniczego posiadanego przez danego użytkownika usług płatniczych u innego dostawcy usług płatniczych albo u więcej niż jednego dostawcy usług płatniczych.

„dostawca usług płatniczych" oznacza podmiot, o którym mowa w art. 1 ust. 1 PSD2[10], lub osobę fizyczną lub prawną korzystającą ze zwolnienia na podstawie art. 32 lub 33 PSD2;

„użytkownik usług płatniczych" oznacza osobę fizyczną lub prawną korzystającą z usługi płatniczej w charakterze płatnika, odbiorcy lub płatnika i odbiorcy;

„dane osobowe" oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

„uwzględnianie ochrony danych w fazie projektowania" odnosi się do środków technicznych i organizacyjnych wbudowanych w produkt lub usługę, zaprojektowanych w celu skutecznej realizacji zasad ochrony danych oraz włączenia do procesu przetwarzania niezbędnych zabezpieczeń, tak by spełnić wymogi RODO oraz chronić prawa osób, których dane dotyczą;

„domyślna ochrona danych" oznacza odpowiednie środki techniczne i organizacyjne wdrożone w ramach produktu lub usługi, które służą zapewnieniu, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania;

„regulacyjny standard techniczny" oznacza rozporządzenie delegowane Komisji (UE) 2018/389 z dnia 27 listopada 2017 r. uzupełniające dyrektywę (UE) 2015/2366 Parlamentu Europejskiego i Rady w odniesieniu do regulacyjnych standardów technicznych dotyczących silnego uwierzytelniania klienta i wspólnych i bezpiecznych otwartych standardów komunikacji;

„dostawcy usług będący osobami trzecimi" oznacza zarówno dostawców świadczących usługę inicjowania płatności, jak i dostawców świadczących usługę dostępu do informacji o rachunku.

1.2 Usługi, o których mowa w PSD2

5. W PSD2 wprowadzono dwa nowe typy (dostawców) usług płatniczych: dostawców świadczących usługę inicjowania płatności i dostawców świadczących usługę dostępu do informacji o rachunku. Załącznik I do PSD2 zawiera osiem usług płatniczych objętych tą dyrektywą.

[10] Art. 1 ust. 1 PSD2 stanowi, że dyrektywa ta ustanawia przepisy, zgodnie z którymi państwa członkowskie rozróżniają następujące kategorie *dostawców usług płatniczych*:
a) instytucje kredytowe zgodnie z definicją w art. 4 ust. 1 pkt 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 575/2013 (1), w tym ich oddziały w rozumieniu art. 4 ust. 1 pkt 17 tego rozporządzenia, gdy takie oddziały znajdują się w Unii, bez względu na to, czy siedziby zarządu tych oddziałów znajdują się w Unii, czy – zgodnie z art. 47 dyrektywy 2013/36/UE i prawem krajowym – poza Unią;
b) instytucje pieniądza elektronicznego w rozumieniu art. 2 pkt 1 dyrektywy 2009/110/WE, w tym – zgodnie z art. 8 tej dyrektywy i prawem krajowym – ich oddziały, gdy takie oddziały znajdują się w Unii, a ich siedziby zarządu znajdują się poza Unią, o ile usługi płatnicze świadczone przez te oddziały są związane z emisją pieniądza elektronicznego;
c) instytucje świadczące żyro pocztowe, które są na mocy prawa krajowego uprawnione do świadczenia usług płatniczych;
d) instytucje płatnicze;
e) EBC i krajowe banki centralne, gdy nie działają one w charakterze organów kształtujących politykę pieniężną lub innych organów publicznych;
f) państwa członkowskie lub ich władze regionalne lub lokalne, gdy nie działają one w charakterze organów publicznych.

6. Dostawcy świadczący usługę inicjowania płatności świadczą usługi polegające na inicjowaniu zleceń płatniczych na wniosek użytkownika usług płatniczych w odniesieniu do rachunku płatniczego użytkownika posiadanego u innego dostawcy usług płatniczych[11]. Dostawca świadczący usługę inicjowania płatności może zwrócić się do dostawcy usług płatniczych prowadzącego rachunek (zazwyczaj banku) o zainicjowanie transakcji w imieniu użytkownika usług płatniczych. Użytkownikiem (usług płatniczych) może być osoba fizyczna (osoba, której dane dotyczą) lub osoba prawna.

7. Dostawcy świadczący usługę dostępu do informacji o rachunku świadczą usługę online polegającą na dostarczaniu skonsolidowanych informacji na temat co najmniej jednego rachunku płatniczego posiadanego przez danego użytkownika usług płatniczych u innego dostawcy usług płatniczych albo u więcej niż jednego dostawcy usług płatniczych[12]. Zgodnie z motywem 28 PSD2 użytkownik usług płatniczych ma możliwość uzyskania w danym momencie natychmiastowego ogólnego obrazu swojej sytuacji finansowej.

8. Jeżeli chodzi o usługi dostępu do informacji o rachunku, może istnieć kilka różnych rodzajów oferowanych usług, z naciskiem na różne funkcje i cele. Na przykład niektórzy dostawcy mogą oferować użytkownikom usługi, takie jak planowanie budżetu i monitorowanie wydatków. Przetwarzanie danych osobowych w kontekście tych usług podlega PSD2. Usługi, które wiążą się z oceną zdolności kredytowej użytkownika usług płatniczych, lub usługi audytu świadczone poprzez gromadzenie informacji za pośrednictwem usługi dostępu do informacji o rachunku, nie wchodzą w zakres PSD2, a zatem podlegają RODO. Ponadto PSD2 nie obejmuje również rachunków innych niż rachunki płatnicze (np. oszczędnościowych, inwestycyjnych). W każdym przypadku RODO stanowi obowiązujące ramy prawne dla przetwarzania danych osobowych.

Przykład 1:

HappyPayments to spółka, która oferuje usługę online polegającą na udostępnianiu informacji o co najmniej jednym rachunku płatniczym za pośrednictwem aplikacji mobilnej w celu monitorowania finansów (usługa dostępu do informacji o rachunku). Dzięki tej usłudze użytkownik usług płatniczych może natychmiast zobaczyć salda i ostatnie transakcje na co najmniej dwóch rachunkach płatniczych w różnych bankach. Na życzenie użytkownika usług płatniczych oferuje ona również klasyfikację wydatków i dochodów według różnych typologii (wynagrodzenie, wypoczynek, energia, kredyt hipoteczny itp.), pomagając w ten sposób użytkownikowi usług płatniczych w zakresie planowania finansowego. W ramach wspomnianej aplikacji HappyPayments oferuje również usługę inicjowania płatności bezpośrednio ze wskazanych przez użytkownika rachunków płatniczych (usługa inicjowania płatności).

9. Z myślą o świadczeniu tych usług w PSD2 uregulowano warunki prawne, na jakich dostawcy świadczący usługę inicjowania płatności i dostawcy świadczący usługę dostępu do informacji o rachunku mogą uzyskiwać dostęp do rachunków płatniczych w celu świadczenia usługi na rzecz użytkownika usług płatniczych.

10. Art. 66 ust. 1 i art. 67 ust. 1 PSD2 stanowią, że użytkownik usług płatniczych ma prawo dostępu do usług płatniczych i usług dostępu do informacji o rachunku oraz prawo do korzystania z tych usług. Oznacza to, że użytkownik usług płatniczych powinien zachować całkowitą swobodę w korzystaniu z tego prawa i nie może być zmuszany do korzystania z niego.

[11] Art. 4 pkt 15 PSD2.
[12] Art. 4 pkt 16 PSD2.

11. Dostęp do rachunków płatniczych i korzystanie z informacji o rachunkach płatniczych uregulowano częściowo w art. 66 i 67 PSD2, zawierających środki ochronne odnoszące się do ochrony danych (osobowych). Art. 66 ust. 3 lit. f) PSD2 stanowi, że dostawca świadczący usługę inicjowania płatności nie żąda od użytkownika usług płatniczych żadnych danych innych niż dane niezbędne do wykonania usługi inicjowania płatności, a art. 66 ust. 3 lit. g) tej dyrektywy stanowi, że dostawcy świadczący usługę inicjowania płatności nie używają, nie uzyskują ani nie przechowują żadnych danych do celów innych niż do wykonania usługi inicjowania płatności wyraźnie zleconej przez płatnika. Ponadto w art. 67 ust. 2 lit. d) PSD2 ograniczono dostęp dostawcy świadczącego usługę dostępu do informacji o rachunku do informacji dotyczących wyznaczonych rachunków płatniczych i związanych z nimi transakcji płatniczych, podczas gdy art. 67 ust. 2 lit. f) tej dyrektywy stanowi, że dostawcy świadczący usługę dostępu do informacji o rachunku nie używają, nie uzyskują ani nie przechowują żadnych danych do celów innych niż do wykonania usługi dostępu do informacji o rachunku wyraźnie zleconej przez użytkownika usług płatniczych, zgodnie z przepisami o ochronie danych. W przepisach tych podkreślono, że w kontekście usług dostępu do informacji o rachunku dane osobowe można gromadzić wyłącznie w konkretnych, wyraźnych i prawnie uzasadnionych celach. Dostawca świadczący usługę dostępu do informacji o rachunku powinien zatem wyraźnie określić w umowie, do jakich konkretnych celów będą przetwarzane dane osobowe dotyczące informacji o rachunku w kontekście świadczonej przez niego usługi dostępu do informacji o rachunku. Umowa powinna być zgodna z prawem, rzetelna i przejrzysta, jak określono w art. 5 RODO, a także zgodna z innymi przepisami dotyczącymi ochrony konsumentów.

12. W zależności od konkretnych okoliczności dostawcy usług płatniczych mogą być administratorami lub podmiotami przetwarzającymi na podstawie RODO. W niniejszych wytycznych „administratorami" są ci dostawcy usług płatniczych, którzy samodzielnie lub wspólnie z innymi określają cele i sposoby przetwarzania danych osobowych. Więcej wskazówek na ten temat można znaleźć w Wytycznych EROD 7/2020 w sprawie pojęć administratora i podmiotu przetwarzającego na gruncie RODO.

2 ZGODNE Z PRAWEM PODSTAWY I DALSZE PRZETWARZANIE NA PODSTAWIE PSD2

2.1 Zgodne z prawem podstawy przetwarzania

13. Zgodnie z RODO administratorzy muszą mieć podstawę prawną, aby przetwarzać dane osobowe. Art. 6 ust. 1 RODO zawiera wyczerpujący i restrykcyjny wykaz sześciu podstaw prawnych przetwarzania danych osobowych zgodnie z RODO[13]. To do administratora należy określenie odpowiedniej podstawy prawnej i zapewnienie spełnienia wszystkich warunków dla tej podstawy prawnej. Określenie, która podstawa jest ważna i najodpowiedniejsza w konkretnej sytuacji, zależy od okoliczności, w jakich odbywa się przetwarzanie, w tym od celu przetwarzania i relacji między administratorem a osobą, której dane dotyczą.

2.2 Art. 6 ust. 1 lit. b RODO (przetwarzanie jest niezbędne do wykonania umowy)

14. Usługi płatnicze świadczy się na podstawie umowy pomiędzy użytkownikiem usług płatniczych a dostawcą usług płatniczych. Jak stwierdzono w motywie 87 PSD2, dyrektywa ta „powinna dotyczyć jedynie umownych zobowiązań i podziału odpowiedzialności między użytkownikiem usług płatniczych a dostawcą usług płatniczych." Zgodnie z RODO główną podstawą prawną przetwarzania danych osobowych w celu świadczenia usług płatniczych jest art. 6 ust. 1 lit. b) RODO, a więc to, że przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy.

15. Usługi płatnicze w ramach PSD2 zdefiniowano w załączniku I do tej dyrektywy. Świadczenie tych usług w rozumieniu PSD2 jest wymogiem zawarcia umowy, w której strony mają dostęp do danych o rachunku płatniczym użytkownika usług płatniczych. Ponadto wspomniani dostawcy usług płatniczych muszą być licencjonowanymi operatorami. W odniesieniu do usług inicjowania płatności i usług dostępu do informacji o rachunku, o których mowa w PSD2, umowy mogą zawierać warunki służące nałożeniu również warunków dotyczących usług dodatkowych, których nie uregulowano w tej dyrektywie. W *Wytycznych EROD 2/2019 w sprawie przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. b) rozporządzenia w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (RODO) w kontekście świadczenia usług online na rzecz osób, których dane dotyczą*, wyjaśniono, że administratorzy muszą ocenić, jakie przetwarzanie danych osobowych jest obiektywnie niezbędne do wykonania umowy. W wytycznych tych wskazano, że uzasadnienie niezbędności zależy od charakteru usługi, wzajemnych interesów i oczekiwań stron umowy, uzasadnienia zawarcia umowy oraz istotnych elementów umowy.

16. W wytycznych EROD 2/2019 wyjaśniono również, że w świetle art. 7 ust. 4 RODO wprowadza się rozróżnienie pomiędzy czynnościami przetwarzania danych niezbędnymi do wykonania umowy a klauzulami uzależniającymi świadczenie usługi od dokonania pewnych czynności przetwarzania, które w rzeczywistości nie są niezbędne do wykonania umowy. „Niezbędne do wykonania" wyraźnie świadczy o tym, że wymaga się czegoś więcej niż tylko klauzuli umownej[14]. Administrator powinien być w stanie wykazać, w jaki sposób główny przedmiot konkretnej umowy zawartej z osobą, której dane dotyczą, nie będzie mógł zostać faktycznie realizowany bez przetwarzania danych osobowych. Samo odniesienie do przetwarzania danych lub wspomnienie o przetwarzaniu danych w umowie nie jest wystarczające, aby takie przetwarzanie objąć zakresem stosowania art. 6 ust. 1 lit. b) RODO.

17. W art. 5 ust. 1 lit. b) RODO przewidziano zasadę ograniczenia celu, zgodnie z którą wymaga się, aby dane osobowe były zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami. Oceniając, czy art. 6 ust. 1 lit. b) stanowi właściwą podstawę prawną w kontekście usługi (płatniczej) online, należy uwzględnić szczególne zamierzenie, cel lub przeznaczenie tej usługi[15]. Cele przetwarzania należy jasno określić i powiadomić o nich osobę, której dane dotyczą, zgodnie z obowiązkami administratora w zakresie ograniczenia celu i przejrzystości. Ocena tego, co jest „niezbędne" obejmuje połączoną, opartą na faktach ocenę przetwarzania „w odniesieniu do zamierzonego celu oraz tego, czy przetwarzanie jest mniej inwazyjne w porównaniu z innymi metodami osiągnięcia tego samego celu". Art. 6 ust. 1 lit. b) nie obejmuje przetwarzania, które jest przydatne, ale nie jest obiektywnie niezbędne do wykonania usługi objętej umową lub podjęcia odpowiednich działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy, nawet jeżeli jest ono niezbędne do innych celów biznesowych administratora[16].

18. W wytycznych EROD 2/2019 wyjaśniono, że w umowie nie można w sposób sztuczny rozszerzać kategorii danych osobowych ani rodzajów operacji przetwarzania, które administrator musi wykonać w celu wykonania umowy w rozumieniu art. 6 ust. 1 lit. b)[17]. Nawiązano w nich również do przypadków, w których może powstawać konieczność zaakceptowania całości umowy bądź jej odrzucenia przez osoby, których dane dotyczą, które mogą być zainteresowane tylko jedną z usług. Może to mieć miejsce, jeżeli administrator zechce połączyć kilka odrębnych usług lub elementów usługi o różnych podstawowych celach, cechach lub przesłankach w ramach jednej umowy. W przypadku gdy umowa obejmuje kilka odrębnych usług lub elementów usługi, które w rzeczywistości można wykonywać niezależnie od siebie, zastosowanie art. 6 ust. 1 lit. b) należy ocenić oddzielnie w kontekście każdej z tych usług, uwzględniając to, co jest obiektywnie

[13] Zgodnie z art. 6 przetwarzanie danych osobowych jest zgodne z prawem, o ile ma zastosowanie co najmniej jeden z poniższych elementów:

(a) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;

(b) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;

(c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;

(d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;

(e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;

(f) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

[14] Wytyczne EROD 2/2019 w sprawie przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. b) RODO w kontekście świadczenia usług online na rzecz osób, których dane dotyczą, s. 8.
[15] Tamże.
[16] Tamże, s. 7.
[17] Tamże, s. 10.

niezbędne do wykonania każdej z poszczególnych usług, których aktywnie zażądała osoba, której dane dotyczą, lub w odniesieniu do których dokonała rejestracji, by z nich korzystać[18].

19. Zgodnie z przytoczonymi wytycznymi administratorzy muszą ocenić, co jest obiektywnie niezbędne do wykonania umowy. Jeżeli administratorzy nie mogą wykazać, że przetwarzanie danych osobowych dotyczących rachunku płatniczego jest obiektywnie niezbędne do świadczenia każdej z tych usług z osobna, art. 6 ust. 1 lit. b) RODO nie stanowi ważnej podstawy prawnej przetwarzania. W takich przypadkach administrator powinien wziąć pod uwagę inną podstawę prawną przetwarzania.

2.3 Zapobieganie nadużyciom

20. Art. 94 ust. 1 PSD2 stanowi, że państwa członkowskie zezwalają na przetwarzanie danych osobowych przez systemy płatności i dostawców usług płatniczych, jeżeli jest to niezbędne, aby zagwarantować zapobieganie oszustwom płatniczym, prowadzenie dochodzeń w ich sprawie i wykrywanie ich. Prawnie uzasadnionym interesem dostawcy usług płatniczych, którego sprawa dotyczy, może być przetwarzanie danych osobowych bezwzględnie niezbędne do zapobiegania oszustwom, o ile charakteru nadrzędnego nie mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą[19]. Czynności przetwarzania w celu zapobiegania nadużyciom powinny opierać się na starannej ocenie poszczególnych przypadków przez administratora zgodnie z zasadą rozliczalności. Ponadto, aby zapobiec nadużyciom, administratorzy mogą również podlegać szczególnym zobowiązaniom prawnym, które wymagają przetwarzania danych osobowych.

2.4 Dalsze przetwarzanie (dostawcy świadczący usługę dostępu do informacji o rachunku i dostawcy świadczący usługę inicjowania płatności)

21. W art. 6 ust. 4 RODO określono warunki przetwarzania danych osobowych w celu innym niż cel, w którym dane osobowe zostały zebrane. Dokładniej rzecz ujmując, takie dalsze przetwarzanie może się odbywać, jeśli opiera się na prawie Unii lub prawie państwa członkowskiego stanowiących w demokratycznym społeczeństwie niezbędny i proporcjonalny środek służący zagwarantowaniu celów, o których mowa w art. 23 ust. 1, w przypadku gdy osoba, której dane dotyczą, wyraziła zgodę lub gdy przetwarzanie w celu innym niż cel, w którym zebrano dane osobowe, jest zgodne z pierwotnym celem.

22. Należy starannie uwzględnić art. 66 ust. 3 lit. g) i art. 67 ust. 2 lit. f) PSD2. Jak wspomniano powyżej, art. 66 ust. 3 lit. g) PSD2 stanowi, że dostawca świadczący usługę inicjowania płatności nie używa, nie uzyskuje ani nie przechowuje żadnych danych do celów innych niż do wykonania usługi inicjowania płatności wyraźnie zleconej przez płatnika. Art. 67 ust. 2 lit. f) PSD2 stanowi, że dostawca świadczący usługę dostępu do informacji o rachunku nie używa, nie uzyskuje ani nie przechowuje żadnych danych do celów innych niż do wykonania usługi dostępu do informacji o rachunku wyraźnie zleconej przez użytkownika usług płatniczych, zgodnie z przepisami o ochronie danych.

23. W związku z tym art. 66 ust. 3 lit. g) i art. 67 ust. 2 lit. f) PSD2 znacznie ograniczają możliwości przetwarzania w innym celu, co oznacza, że przetwarzanie w innym celu jest niedozwolone, chyba że osoba, której dane dotyczą, wyraziła zgodę zgodnie z art. 6 ust. 1 lit. a) RODO lub przetwarzanie przewidziano w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator, zgodnie z art. 6 ust. 4 RODO. Jeżeli przetwarzanie w celu innym niż cel, w którym dane osobowe zostały zebrane, nie odbywa się na podstawie zgody osoby, której dane dotyczą, ani prawa Unii lub prawa państwa członkowskiego, ograniczenia określone w art. 66 ust. 3 lit. g) i art. 67 ust. 2 lit. f) PSD2 wyraźnie wskazują, że jakikolwiek inny cel nie jest zgodny z celem, w którym dane osobowe zostały pierwotnie zebrane. W oparciu o test zgodności, o którym mowa w art. 6 ust. 4 RODO, nie można stwierdzić podstawy prawnej przetwarzania danych.

24. Art. 6 ust. 4 RODO umożliwia dalsze przetwarzanie na podstawie prawa Unii lub prawa państwa członkowskiego. Na przykład wszyscy dostawcy świadczący usługę inicjowania płatności i dostawcy świadczący usługę dostępu do informacji o rachunku są podmiotami zobowiązanymi zgodnie z art. 3 pkt 2 lit. a) dyrektywy Parlamentu Europejskiego i Rady (UE) 2015/849 z dnia 20 maja 2015 r. w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu (czwartej dyrektywy w sprawie przeciwdziałania praniu pieniędzy). Te podmioty zobowiązane są zatem zmuszone do stosowania środków należytej staranności wobec klienta określonych w dyrektywie. Dane osobowe przetwarzane w związku z usługą objętą zakresem PSD2 są w związku z tym przetwarzane dalej na podstawie co najmniej jednego zobowiązania prawnego spoczywającego na dostawcy usług[20].

25. Jak wspomniano w pkt 20, z art. 6 ust. 4 RODO wynika, że przetwarzanie w celu innym niż cel, w którym dane osobowe zostały zebrane, może opierać się na zgodzie osoby, której dane dotyczą, jeśli spełniono wszystkie warunki wyrażenia zgody określone w RODO. Jak określono powyżej, administrator musi wykazać, że istnieje możliwość odmowy lub wycofania zgody bez niekorzystnych konsekwencji (motyw 42 RODO).

2.5 Zgodna z prawem podstawa udzielenia dostępu do rachunku (dostawcy usług płatniczych prowadzący rachunek)

26. Jak wspomniano w pkt 10, użytkownicy usług płatniczych mogą realizować prawo do korzystania z usług inicjowania płatności i usług dostępu do informacji o rachunku. Obowiązki nałożone na państwa członkowskie w art. 66 ust. 1 i art. 67 ust. 1 PSD2 należy wdrożyć do prawa krajowego w celu zagwarantowania skutecznego stosowania prawa użytkownika usług płatniczych do korzystania z wyżej wymienionych usług płatniczych. Skuteczne stosowanie takich praw nie byłoby możliwe bez istnienia spoczywającego na dostawcy usług płatniczych prowadzącym rachunek, zazwyczaj banku, powiązanego obowiązku udzielenia dostawcy usług płatniczych dostępu do rachunku, pod warunkiem że spełnił on wszystkie wymogi niezbędne do uzyskania dostępu do rachunku użytkownika usług płatniczych. Ponadto art. 66 ust. 5 i art. 67 ust. 4 PSD2 stanowią wyraźnie, że świadczenia usług inicjowania płatności oraz usług dostępu do informacji o rachunku nie można uzależniać od istnienia stosunku umownego pomiędzy dostawcą świadczącym usługę inicjowania płatności/dostawcą świadczącym usługę dostępu do informacji o rachunku a dostawcą usług płatniczych prowadzącym rachunek.

27. Przetwarzanie danych osobowych przez dostawcę usług płatniczych prowadzącego rachunek polegające na udostępnieniu danych osobowych na żądanie dostawcy świadczącego usługę inicjowania płatności i dostawcy świadczącego usługę dostępu do informacji o rachunku w celu świadczenia przez nich usługi płatniczej na rzecz użytkownika usług płatniczych wynika z obowiązku prawnego. Aby osiągnąć cele określone w PSD2, dostawcy usług płatniczych prowadzący rachunek muszą dostarczać dane osobowe na potrzeby usług świadczonych przez dostawców świadczących usługę inicjowania płatności i dostawców świadczących usługę dostępu do informacji o rachunku, co jest warunkiem koniecznym do świadczenia usług przez tych

[18] Tamże, s. 11.
[19] Motyw 47 RODO.

[20] Należy zauważyć, że dokładna analiza tego, czy dyrektywa w sprawie przeciwdziałania praniu pieniędzy odpowiada normie określonej w art. 6 ust. 4 RODO, wykracza poza zakres niniejszego dokumentu.

dostawców, a tym samym zapewnienia praw przewidzianych w art. 66 ust. 1 i art. 67 ust. 1 PSD2. W związku z tym właściwą podstawą prawną w tym przypadku jest art. 6 ust. 1 lit. c) RODO.

28. Ponieważ w RODO określono, że przetwarzanie na podstawie obowiązku prawnego powinno być wyraźnie uregulowane prawem Unii lub prawem państwa członkowskiego (zob. art. 6 ust. 3 RODO), obowiązek udzielenia dostępu przez dostawców usług płatniczych prowadzących rachunek powinien wynikać z prawa krajowego transponującego PSD2.

3 WYRAŹNA ZGODA

3.1 Zgoda w rozumieniu RODO

29. Zgodnie z RODO zgoda stanowi jedną z sześciu podstaw prawnych zgodności przetwarzania danych osobowych z prawem. Art. 4 ust. 11 RODO definiuje zgodę jako „dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych". Te cztery warunki, „dobrowolne, konkretne, świadome i jednoznaczne", są niezbędne dla ważności zgody. Zgodnie ze sporządzonymi przez EROD Wytycznymi 05/2020 dotyczącymi zgody na mocy rozporządzenia 2016/679 zgoda może być właściwą, zgodną z prawem podstawą wyłącznie wówczas, gdy osobie, której dane dotyczą, zapewnia się kontrolę oraz rzeczywistą możliwość wyboru w odniesieniu do przyjęcia lub odrzucenia zaoferowanych warunków lub odrzucenia ich bez niekorzystnych konsekwencji. Zwracając się o zgodę, administrator ma obowiązek oceny, czy spełni wszystkie wymogi uzyskania ważnej zgody. Zgoda uzyskana w pełnej zgodności z RODO jest narzędziem zapewniającym osobom, których dane dotyczą, kontrolę nad tym, czy dotyczące ich dane osobowe będą przetwarzane. W braku zgodności zgody z RODO kontrola ze strony osoby, której dane dotyczą, staje się złudna, a zgoda będzie nieważną podstawą prawną przetwarzania, co spowoduje niezgodność z prawem czynności przetwarzania[21].

30. RODO zawiera również dalsze zabezpieczenia opisane w art. 7, który stanowi, że administrator musi być w stanie wykazać, że w chwili przetwarzania danych dysponował ważną zgodą. Ponadto zapytanie o zgodę musi zostać przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem. Oprócz tego osoba, której dane dotyczą, musi zostać poinformowana o prawie do wycofania zgody w dowolnym momencie, przy czym takie wycofanie zgody musi być równie łatwe jak jej wyrażenie.

31. Zgodnie z art. 9 RODO zgoda jest jednym z wyjątków od ogólnego zakazu przetwarzania szczególnych kategorii danych osobowych. W takim przypadku zgoda osoby, której dane dotyczą, musi być jednak „wyraźna"[22].

32. Zgodnie ze sporządzonymi przez EROD Wytycznymi 05/2020 dotyczącymi zgody na mocy rozporządzenia 2016/679 wyraźna zgoda, o której mowa w RODO, odnosi się do sposobu wyrażenia zgody przez osobę, której dane dotyczą. Oznacza to, że osoba, której dane dotyczą, powinna złożyć w sposób wyraźny oświadczenie o wyrażeniu zgody na określony cel lub określone cele przetwarzania. Oczywistym sposobem zapewnienia, aby zgoda była wyraźna, byłoby jej wyraźne potwierdzenie w pisemnym oświadczeniu. W stosownych przypadkach administrator mógłby zapewnić podpisanie pisemnego oświadczenia przez osobę, której dane dotyczą, aby rozwiać wszelkie możliwe wątpliwości i zapobiec możliwemu brakowi dowodów w przyszłości.

33. W żadnym wypadku zgoda nie może być wywnioskowana z potencjalnie niejednoznacznych oświadczeń lub działań. Administrator musi również mieć świadomość, że zgody nie można uzyskać w drodze tej samej czynności co zawarcie umowy czy zaakceptowanie ogólnych warunków usługi.

3.2 Zgoda w rozumieniu PSD2

[21] EROD, Wytyczne 05/2020 dotyczące zgody na mocy rozporządzenia 2016/679, pkt 3.
[22] Zob. także opinia 15/2011 w sprawie definicji zgody (WP 187), s. 6–8, lub opinia 06/2014 w sprawie pojęcia uzasadnionych interesów administratora danych zawartego w art. 7 dyrektywy 95/46/WE (WP 217), s. 9, 10, 13 i 14.

34. EROD zauważa, że ramy prawne dotyczące wyraźnej zgody są skomplikowane, ponieważ pojęcie „wyraźnej zgody" znajduje się zarówno w PSD2, jak i w RODO. Nasuwa się pytanie, czy „wyraźną zgodę", o której mowa w art. 94 ust. 2 PSD2, należy interpretować w taki sam sposób jak wyraźną zgodę na mocy RODO.

3.2.1 Wyraźna zgoda w rozumieniu art. 94 ust. 2 PSD2

35. PSD2 zawiera szereg szczegółowych zasad dotyczących przetwarzania danych osobowych, w szczególności w art. 94 ust. 1, który stanowi, że przetwarzanie danych osobowych na potrzeby PSD2 musi odbywać się zgodnie z unijnymi przepisami o ochronie danych. Ponadto art. 94 ust. 2 PSD2 stanowi, że dostawcy usług płatniczych uzyskują dostęp jedynie do danych osobowych niezbędnych do świadczenia swoich usług płatniczych, przetwarzają te dane i zatrzymują je za wyraźną zgodą użytkownika usług płatniczych. Zgodnie z art. 33 ust. 2 PSD2 wymóg wyraźnej zgody użytkownika usług płatniczych nie ma zastosowania do dostawców świadczących usługę dostępu do informacji o rachunku. W art. 67 ust. 2 lit. a) PSD2 przewiduje się jednak konieczność uzyskania wyraźnej zgody na świadczenie usługi przez dostawców świadczących usługę dostępu do informacji o rachunku.

36. Jak wspomniano powyżej, lista zgodnych z prawem podstaw przetwarzania na podstawie RODO jest wyczerpująca. Jak wspomniano w pkt 14, podstawą prawną przetwarzania danych osobowych w celu świadczenia usług płatniczych jest zasadniczo art. 6 ust. 1 lit. b) RODO, a więc to, że przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy. Wynika z tego, że art. 94 ust. 2 PSD2 nie można uznać za dodatkową podstawę prawną przetwarzania danych osobowych. EROD uważa, że w związku z powyższym ustęp ten należy interpretować z jednej strony zgodnie z mającymi zastosowanie ramami prawnymi ochrony danych, a z drugiej strony w sposób zachowujący jego skuteczność. Wyraźną zgodę w rozumieniu art. 94 ust. 2 PSD2 należy zatem uznać za dodatkowy wymóg o charakterze umownym[23] w odniesieniu do dostępu do danych osobowych, a następnie ich przetwarzania i przechowywania na potrzeby świadczenia usług płatniczych, a zatem taka zgoda nie jest tożsama z (wyraźną) zgodą na podstawie RODO.

37. „Wyraźna zgoda", o której mowa w art. 94 ust. 2 PSD2, jest zgodą umowną. Oznacza to, że art. 94 ust. 2 PSD2 należy interpretować w ten sposób, że zawierając umowę z dostawcą usług płatniczych na podstawie tej dyrektywy, osoby, których dane dotyczą, muszą być w pełni świadome szczególnych kategorii danych osobowych, które będą przetwarzane. Ponadto należy poinformować je o konkretnym celu (usługa płatnicza), w którym ich dane osobowe będą przetwarzane, i muszą one wyraźnie zgodzić się na te klauzule. Klauzule takie powinny wyraźnie odróżniać się od pozostałych kwestii poruszanych w umowie, a osoba, której dane dotyczą, musiałaby wyraźnie je zaakceptować.

38. Kluczowym elementem w kontekście pojęcia „wyraźnej zgody" w rozumieniu art. 94 ust. 2 PSD2 jest uzyskanie dostępu do danych osobowych w celu późniejszego przetwarzania i przechowywania tych danych na potrzeby świadczenia usług płatniczych. Oznacza to, że dostawca usług płatniczych[24] nie przetwarza jeszcze danych osobowych, ale potrzebuje dostępu do danych osobowych, które przetwarzano na odpowiedzialność innego administratora. Jeśli użytkownik usług płatniczych zawiera umowę na przykład z dostawcą świadczącym usługę inicjowania płatności, dostawca ten musi uzyskać dostęp do danych osobowych użytkownika usług płatniczych, za których przetwarzanie odpowiedzialny jest dostawca usług płatniczych prowadzący rachunek.

[23] Pismo EROD w sprawie drugiej dyrektywy w sprawie usług płatniczych, 5 lipca 2018 r., s. 4.
[24] Dotyczy to usług 1–7 wymienionych w załączniku I do PSD2.

Przedmiotem wyraźnej zgody, o której mowa w art. 94 ust. 2 PSD2, jest zezwolenie na uzyskanie dostępu do tych danych osobowych w celu umożliwienia przetwarzania i przechowywania tych danych osobowych, które są niezbędne w celu świadczenia usługi płatniczej. W przypadku wyrażenia wyraźnej zgody przez osobę, której dane dotyczą, dostawca usług płatniczych prowadzący rachunek zobowiązany jest do udzielenia dostępu do wskazanych danych osobowych.

39. Mimo że zgoda, o której mowa w art. 94 ust. 2 PSD2, nie stanowi podstawy prawnej przetwarzania danych osobowych, jest ona szczególnie związana z danymi osobowymi i ochroną danych oraz zapewnia przejrzystość i pewien stopień kontroli dla użytkownika usług płatniczych[25]. Chociaż w PSD2 nie określono materialnych przesłanek zgody, o której mowa w art. 94 ust. 2 tej dyrektywy, należy ją, jak stwierdzono powyżej, rozumieć zgodnie z mającymi zastosowanie ramami prawnymi ochrony danych oraz w sposób pozwalający zachować jej skuteczność.

40. W odniesieniu do informacji, które mają być dostarczane przez administratorów, i wymogu przejrzystości w Wytycznych Grupy Roboczej Art. 29 w sprawie przejrzystości stwierdzono, że „[n]ajważniejszym aspektem zasady przejrzystości, którą określono we wspomnianych przepisach, jest to, że osoba, której dane dotyczą, powinna zawsze być w stanie z wyprzedzeniem określić zakres i skutki przetwarzania i że nie powinna zostać później zaskoczona informacją, w jaki sposób wykorzystano jej dane osobowe"[26].

41. Ponadto zgodnie z zasadą ograniczenia celu dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach (art. 5 ust. 1 lit. b) RODO). Jeśli dane osobowe gromadzi się w więcej niż jednym celu, „administratorzy powinni unikać określania wyłącznie jednego ogólnego celu, aby uzasadnić różne czynności dalszego przetwarzania, które w rzeczywistości są tylko w niewielkim stopniu związane z rzeczywistym pierwotnym celem"[27]. EROD podkreśliła, ostatnio w kontekście umów dotyczących usług online, ryzyko związane z zawieraniem w umowach warunków ogólnych przetwarzania i stwierdziła, że cel zbierania danych musi być jasno i konkretnie określony: powinien być wystarczająco szczegółowy, aby określić, jaki rodzaj przetwarzania danych jest objęty określonym celem, a jaki nie jest, oraz aby umożliwić ocenę zgodności z prawem i zastosowanie zabezpieczeń ochrony danych[28].

42. W kontekście dodatkowego wymogu dotyczącego wyraźnej zgody zgodnie z art. 94 ust. 2 PSD2 oznacza to, że administratorzy muszą udzielić osobom, których dane dotyczą, konkretnych i wyraźnych informacji o określonych przez administratora konkretnych celach, w których ich dane osobowe są udostępniane, przetwarzane i zatrzymywane. Zgodnie z art. 94 ust. 2 PSD2, osoby, których dane dotyczą, muszą wyraźnie zaakceptować te konkretne cele.

43. Ponadto, jak wskazano w pkt 10 powyżej, EROD podkreśla, że użytkownik usług płatniczych musi mieć możliwość wyboru, czy chce korzystać z danej usługi czy nie, i nie może być do tego zmuszany. Zgoda, o której mowa w art. 94 ust. 2 PSD2, musi być również zgodą wyrażoną dobrowolnie.

3.3 Podsumowanie

[25] Art. 94 ust. 2 PSD2 wchodzi w zakres rozdziału 4 „Ochrona danych".
[26] Wytyczne Grupy Roboczej Art. 29 w sprawie przejrzystości na podstawie rozporządzenia 2016/679, pkt 10 (przyjęte w dniu 11 kwietnia 2018 r.) – zatwierdzone przez EROD.
[27] Opinia Grupy Roboczej Art. 29 03/2013 w sprawie ograniczenia celu (WP203), s. 16.
[28] Wytyczne 2/2019 w sprawie przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. b) rozporządzenia w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (RODO) w kontekście świadczenia usług online na rzecz osób, których dane dotyczą, pkt 16 (wersja do konsultacji publicznych) oraz opinia 03/2013 Grupy Roboczej Art. 29 w sprawie ograniczenia celu (WP203), s. 15–16.

44. Wyraźna zgoda w rozumieniu PSD2 różni się od (wyraźnej) zgody w rozumieniu RODO. Wyraźna zgoda na podstawie art. 94 ust. 2 PSD2 jest dodatkowym wymogiem o charakterze umownym. Jeśli dostawca usług płatniczych potrzebuje dostępu do danych osobowych w celu świadczenia usługi płatniczej, zgodnie z art. 94 ust. 2 PSD2 konieczna jest wyraźna zgoda użytkownika usług płatniczych.

4 PRZETWARZANIE DANYCH MILCZĄCEJ STRONY

4.1 Dane milczącej strony

45. Kwestią związaną z ochroną danych, która wymaga starannego uwzględnienia, jest przetwarzanie tak zwanych danych milczącej strony. W kontekście niniejszego dokumentu dane milczącej strony to dane osobowe osoby, której dane dotyczą, która nie jest użytkownikiem określonego dostawcy usług płatniczych, ale której dane osobowe są przetwarzane przez tego określonego dostawcę usług płatniczych w celu wykonania umowy między dostawcą a użytkownikiem usług płatniczych. Dzieje się tak na przykład w przypadku, gdy użytkownik usług płatniczych, osoba A, której dane dotyczą, korzysta z usług dostawcy świadczącego usługę dostępu do informacji o rachunku, a osoba B, której dane dotyczą, dokonała serii transakcji płatniczych na rachunek płatniczy osoby A, której dane dotyczą. W tym przypadku osobę B, której dane dotyczą, uważa się za „milczącą stronę", a dane osobowe (takie jak numer rachunku osoby B, której dane dotyczą, i kwota będąca przedmiotem tych transakcji) osoby B, której dane dotyczą, uważa się za „dane milczącej strony".

4.2 Prawnie uzasadniony interes administratora

46. W art. 5 ust. 1 lit. b) RODO zawarto wymóg, aby dane osobowe były wyłącznie zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i aby nie można było przetwarzać ich dalej w sposób niezgodny z tymi celami. Ponadto w RODO wymaga się, aby wszelkie przetwarzanie danych osobowych było zarówno niezbędne, jak i proporcjonalne oraz zgodne z zasadami ochrony danych, takimi jak zasada ograniczenia celu i zasada minimalizacji danych.

47. Przetwarzanie danych milczącej strony na podstawie RODO jest możliwe, gdy przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią (art. 6 ust. 1 lit. f) RODO). Takie przetwarzanie może mieć jednak miejsce jedynie wówczas, gdy wobec prawnie uzasadnionego interesu realizowanego przez administratora „nadrzędnego charakteru nie mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych".

48. Podstawą prawną przetwarzania danych milczącej strony przez dostawców świadczących usługę inicjowania płatności i dostawców świadczących usługę dostępu do informacji o rachunku – w kontekście świadczenia usług płatniczych na podstawie PSD2 – może być zatem prawnie uzasadniony interes administratora lub strony trzeciej, polegający na wykonaniu umowy z użytkownikiem usług płatniczych. Konieczność przetwarzania danych osobowych milczącej strony jest ograniczona i ustalana na podstawie rozsądnych oczekiwań tych osób, których dane dotyczą. W kontekście świadczenia usług płatniczych objętych PSD2 należy ustanowić skuteczne i odpowiednie środki w celu zagwarantowania, że interesy lub podstawowe prawa i wolności milczących stron będą miały nadrzędny charakter, oraz w celu zapewnienia poszanowania rozsądnych oczekiwań osób, których dane dotyczą, w odniesieniu do przetwarzania ich danych osobowych. W tym względzie administrator (dostawca świadczący usługę dostępu do informacji o rachunku lub dostawca świadczący usługę inicjowania płatności) musi ustanowić niezbędne zabezpieczenia w zakresie przetwarzania danych w celu ochrony praw osób, których dane dotyczą. Obejmuje to środki techniczne zapewniające, aby danych milczącej strony nie przetwarzano w celu innym niż cel, w którym dane osobowe zostały pierwotnie zebrane przez dostawców świadczących usługę inicjowania płatności i dostawców świadczących usługę dostępu do informacji o rachunku. Jeśli jest to wykonalne, należy również zastosować szyfrowanie lub inne techniki w celu osiągnięcia odpowiedniego poziomu bezpieczeństwa i minimalizacji danych.

4.3 Dalsze przetwarzanie danych osobowych milczącej strony

49. Jak stwierdzono w pkt 29, dane osobowe przetwarzane w związku z usługą płatniczą uregulowaną w PSD2 mogłyby być przetwarzane dalej na podstawie zobowiązań prawnych spoczywających na dostawcy usług. Wspomniane zobowiązania prawne mogłyby dotyczyć danych osobowych milczącej strony.

50. W odniesieniu do dalszego przetwarzania danych milczącej strony na podstawie prawnie uzasadnionego interesu EROD jest zdania, że dane te nie mogą być wykorzystywane w celu innym niż cel, w którym dane osobowe zostały zebrane, chyba że odbywa się to na podstawie prawa Unii lub państwa członkowskiego. Uzyskanie zgody milczącej strony jest niewykonalne z prawnego punktu widzenia, ponieważ w celu uzyskania takiej zgody konieczne byłoby zbieranie lub przetwarzanie danych osobowych milczącej strony, dla których to działań nie można znaleźć podstawy prawnej w art. 6 RODO. W oparciu o test zgodności, o którym mowa w art. 6 ust. 4 RODO, również nie można stwierdzić podstawy przetwarzania danych do innych celów (np. działań z zakresu marketingu bezpośredniego). Prawa i wolności tych milczących stron będących osobami, których dane dotyczą, nie będą przestrzegane, jeżeli nowy administrator wykorzysta dane osobowe do innych celów, biorąc pod uwagę kontekst, w jakim zebrano dane osobowe, w szczególności: brak jakiegokolwiek związku z osobami, których dane dotyczą, będącymi milczącymi stronami[29]; brak związku pomiędzy jakimkolwiek innym celem a celem, w którym dane osobowe zostały pierwotnie zebrane (tj. fakt, że dostawcy usług płatniczych potrzebują danych milczącej strony wyłącznie w celu wykonania umowy z drugą umawiającą się stroną); charakter przedmiotowych danych osobowych[30], okoliczność, że osoby, których dane dotyczą, nie mają rozsądnych przesłanek, by spodziewać się dalszego przetwarzania, lub nawet mogą nie być świadome, który administrator może przetwarzać ich dane osobowe, oraz biorąc pod uwagę ograniczenia prawne dotyczące przetwarzania określone w art. 66 ust. 3 lit. g) i w art. 67 ust. 2 lit. f) PSD2.

[29] Motyw 87 PSD2 stanowi, że dyrektywa ta dotyczy jedynie „umownych zobowiązań i podziału odpowiedzialności między użytkownikiem usług płatniczych a dostawcą usług płatniczych". Dane milczącej strony nie są zatem objęte zakresem PSD2.

[30] Należy zachować szczególną ostrożność przy przetwarzaniu finansowych danych osobowych, ponieważ zgodnie z wytycznymi dotyczącymi oceny skutków dla ochrony danych przetwarzanie to można uznać za zwiększające możliwe ryzyko naruszenia praw i wolności osób.

5 PRZETWARZANIE SZCZEGÓLNYCH KATEGORII DANYCH OSOBOWYCH NA PODSTAWIE PSD2

5.1 Szczególne kategorie danych osobowych

51. Zgodnie z art. 9 ust. 1 RODO zabrania się „przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby".

52. Należy podkreślić, że w niektórych państwach członkowskich płatności elektroniczne są już powszechne i wiele osób preferuje je zamiast gotówki w codziennych transakcjach. Jednocześnie transakcje finansowe mogą ujawniać informacje szczególnie chronione o konkretnej osobie, której danej dotyczą, w tym informacje dotyczące szczególnych kategorii danych osobowych. Na przykład, w zależności od szczegółów transakcji, na podstawie darowizn przekazywanych na rzecz partii lub organizacji politycznych, kościołów lub parafii mogą zostać ujawnione poglądy polityczne i przekonania religijne. Na podstawie potrącania rocznej składki członkowskiej z rachunku bankowego danej osoby może zostać ujawnione jej członkostwo w związku zawodowym. Na podstawie analizy rachunków opłacanych przez osobę, której dane dotyczą, na rzecz lekarza (np. psychiatry) mogą być zbierane dane osobowe dotyczące zdrowia. Ponadto informacje dotyczące określonych zakupów mogą ujawniać informacje o seksualności osoby lub jej orientacji seksualnej. Jak wynika z tych przykładów, każda transakcja może zawierać szczególne kategorie danych osobowych. Ponadto usługi dostępu do informacji o rachunku mogą opierać się na profilowaniu zdefiniowanym w art. 4 pkt 4 RODO. Jak stwierdzono uprzednio w sporządzonych przez Grupę Roboczą Art. 29 i zatwierdzonych przez EROD Wytycznych w sprawie zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania do celów rozporządzenia 2016/679/UE, „[p]rofilowanie może doprowadzić do stworzenia danych szczególnej kategorii wskutek ich wywnioskowania z danych, które same w sobie nie są danymi szczególnej kategorii, ale które stają się nimi w momencie ich połączenia z innymi danymi"[31]. Oznacza to, że na podstawie sumy transakcji finansowych mogą zostać ujawnione różne wzorce zachowań, które mogą obejmować szczególne kategorie danych osobowych. Istnieje zatem duże prawdopodobieństwo, że dostawca usług przetwarzający informacje dotyczące transakcji finansowych osób, których dane dotyczą, przetwarza również szczególne kategorie danych osobowych.

53. W odniesieniu do terminu „szczególnie chronione dane dotyczące płatności" EROD zauważa, co następuje. Definicja szczególnie chronionych danych dotyczących płatności zawarta w PSD2 różni się znacząco od sposobu, w jaki termin „dane wrażliwe" jest powszechnie stosowany w kontekście RODO i (przepisów dotyczących) ochrony danych. Podczas gdy w PSD2 „szczególnie chronione dane dotyczące płatności" zdefiniowano jako „dane, w tym indywidualne dane uwierzytelniające, które mogą być wykorzystywane do dokonywania oszustw", w RODO podkreśla się potrzebę szczególnej ochrony szczególnych kategorii danych osobowych, które – zgodnie z art. 9 RODO – z racji swego charakteru są szczególnie wrażliwe w świetle podstawowych praw i wolności[32]. W związku z tym zaleca się co najmniej określenie, jakiego rodzaju dane osobowe będą

[31] Grupa Robocza ds. Ochrony Osób Fizycznych w zakresie Przetwarzania Danych Osobowych, Wytyczne w sprawie zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania do celów rozporządzenia 2016/679/UE, WP251rev.01, s. 15.

[32] Na przykład w motywie 10 RODO szczególne kategorie danych osobowych określa się jako „dane wrażliwe".

przetwarzane, oraz wskazanie kategorii tych danych. Najprawdopodobniej konieczne będzie przeprowadzenie oceny skutków dla ochrony danych zgodnie z art. 35 RODO, która pomoże w takiej identyfikacji. Więcej wytycznych dotyczących oceny skutków dla ochrony danych można znaleźć w sporządzonych przez Grupę Roboczą Art. 29 Wytycznych dotyczących oceny skutków dla ochrony danych oraz pomagających ustalić, czy przetwarzanie „może powodować wysokie ryzyko" do celów rozporządzenia 2016/679, zatwierdzone przez EROD.

5.2 Możliwe wyjątki

54. Zakaz zawarty w art. 9 RODO nie jest bezwzględny. W szczególności, o ile wyjątki określone w art. 9 ust. 2 lit. b)–f) i h)–j) RODO wyraźnie nie mają zastosowania do przetwarzania danych osobowych w kontekście PSD2, można rozważyć dwa wyjątki przewidziane w art. 9 ust. 2 RODO:

a) Zakaz nie ma zastosowania w przypadku, gdy osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach (art. 9 ust. 2 lit. a) RODO).

b) Zakaz nie ma zastosowania w przypadku, gdy przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą (art. 9 ust. 2 lit. g) RODO).

55. Należy zauważyć, że wykaz wyjątków przewidzianych w art. 9 ust. 2 RODO jest wyczerpujący. Dostawca usług musi uznać możliwość włączenia szczególnych kategorii danych osobowych do danych osobowych przetwarzanych w celu świadczenia usług objętych zakresem PSD2. Ponieważ zakaz zawarty w art. 9 ust. 1 RODO ma zastosowanie do tych dostawców usług, muszą oni upewnić się, że w ich przypadku zastosowanie ma jeden z wyjątków przewidzianych w art. 9 ust. 2 RODO. Należy podkreślić, że w przypadku gdy usługodawca nie może wykazać, że spełniono warunki jednego z wyjątków, zakaz zawarty w art. 9 ust. 1 ma zastosowanie.

5.3 Ważny interes publiczny

56. Usługi płatnicze mogą obejmować przetwarzanie szczególnych kategorii danych osobowych ze względów związanych z ważnym interesem publicznym, ale jedynie w przypadku, gdy spełniono wszystkie warunki określone w art. 9 ust. 2 lit. g) RODO. Oznacza to, że przetwarzanie szczególnych kategorii danych osobowych musi zostać uregulowane w szczególnym wyjątku od art. 9 ust. 1 RODO w prawie Unii lub państwa członkowskiego. Przepis ten będzie musiał uwzględniać proporcjonalność w stosunku do zamierzonego celu przetwarzania oraz zawierać odpowiednie i konkretne środki ochrony praw podstawowych i interesów osób, których dane dotyczą. Ponadto taki przepis na mocy prawa Unii lub prawa państwa członkowskiego będzie musiał respektować istotę prawa do ochrony danych. Co więcej, należy również wykazać, że przetwarzanie szczególnych kategorii danych jest niezbędne ze względu na ważny interes publiczny, w tym interesy o znaczeniu systemowym. Dopiero gdy wszystkie te warunki zostaną w pełni spełnione, wyjątek ten będzie mógł mieć zastosowanie do określonych rodzajów usług płatniczych.

5.4 Wyraźna zgoda

57. W przypadkach, w których wyjątek przewidziany w art. 9 ust. 2 lit. g) RODO nie ma zastosowania, wydaje się, że uzyskanie wyraźnej zgody zgodnie z warunkami ważnej zgody określonymi w RODO pozostaje jedynym możliwym zgodnym z prawem wyjątkiem w odniesieniu do przetwarzania szczególnych kategorii danych osobowych przez dostawców usług będących osobami trzecimi. W

Wytycznych 05/2020 dotyczących zgody na mocy rozporządzenia 2016/679 EROD stwierdza się[33], że „[w] art. 9 ust. 2 nie przewidziano, by charakter danych »niezbędnych do wykonania umowy« był wyjątkiem od ogólnego zakazu przetwarzania szczególnych kategorii danych. W związku z tym administratorzy i państwa członkowskie, które znajdują się w takiej sytuacji, powinni zbadać konkretne wyjątki przewidziane w art. 9 ust. 2 lit. b)–j)". Jeżeli dostawcy usług opierają się na art. 9 ust. 2 lit. a) RODO, muszą upewnić się, że przed przystąpieniem do przetwarzania uzyskali wyraźną zgodę. Wyraźna zgoda, o której mowa w art. 9 ust. 2 lit. a) RODO, musi spełniać wszystkie wymogi RODO.

5.5 Brak odpowiedniego wyjątku

58. Jak zauważono powyżej, gdy usługodawca nie może wykazać, że spełniono warunki jednego z wyjątków, zakaz zawarty w art. 9 ust. 1 ma zastosowanie. W takim przypadku można wprowadzić środki techniczne, aby zapobiec przetwarzaniu szczególnych kategorii danych osobowych, na przykład poprzez uniemożliwienie przetwarzania niektórych punktów danych. W tym względzie dostawcy usług płatniczych mogą zbadać techniczne możliwości wyłączenia szczególnych kategorii danych osobowych i umożliwienia wybranego dostępu, co zapobiegłoby przetwarzaniu szczególnych kategorii danych osobowych dotyczących milczących stron przez dostawców usług będących osobami trzecimi.

[33] EROD, Wytyczne 05/2020 dotyczące zgody na mocy rozporządzenia 2016/679, pkt 99.

6 MINIMALIZACJA DANYCH, BEZPIECZEŃSTWO, PRZEJRZYSTOŚĆ, ROZLICZALNOŚĆ I PROFILOWANIE

6.1 Minimalizacja danych i uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych

59. Zasada minimalizacji danych jest zapisana w art. 5 ust. 1 lit. c) RODO: „Dane osobowe muszą być [...] adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane". Zasadniczo, zgodnie z zasadą minimalizacji danych, administratorzy nie powinni przetwarzać więcej danych osobowych niż jest to konieczne do osiągnięcia danego celu. Jak wskazano w rozdziale 2, ilość i rodzaj danych osobowych niezbędnych do świadczenia usługi płatniczej określa się na podstawie obiektywnego i wspólnie uzgodnionego celu umowy[34]. Minimalizacja danych ma zastosowanie przy każdym przetwarzaniu (np. przy każdym zbieraniu danych osobowych, dostępie do nich i ich żądaniu). W Wytycznych 4/2019 dotyczących artykułu 25 Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrony danych z EROD stwierdza, że „podmioty przetwarzające i dostawców technologii również uznaje się za kluczowe podmioty umożliwiające uwzględnianie ochrony danych w fazie projektowania oraz domyślną ochronę danych; powinni oni również mieć świadomość, że administratorzy są zobowiązani do przetwarzania danych osobowych wyłącznie za pomocą systemów i technologii, które mają wbudowany mechanizm ochrony danych"[35].

60. Art. 25 RODO zawiera obowiązki uwzględniania ochrony danych w fazie projektowania oraz domyślnej ochrony danych. Obowiązki te mają szczególne znaczenie dla zasady minimalizacji danych. Artykuł ten stanowi, że administratorzy – zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania – wdrażają odpowiednie środki techniczne i organizacyjne, zaprojektowane w celu skutecznej realizacji zasad ochrony danych oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi RODO oraz chronić prawa osób, których dane dotyczą. Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. Środki te mogą obejmować szyfrowanie, pseudonimizację i inne środki techniczne.

61. W przypadku stosowania obowiązku wynikającego z art. 25 RODO elementami, które należy uwzględnić, są stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze, jakie stwarza przetwarzanie. Dalsze wyjaśnienia dotyczące tego obowiązku znajdują się we wspomnianych wyżej Wytycznych EROD 4/2019 w sprawie uwzględniania ochrony danych w fazie projektowania oraz domyślnej ochrony danych z art. 25.

6.2 Środki minimalizacji danych

62. Dostawca usług będący osobą trzecią uzyskujący dostęp do danych rachunku płatniczego w celu świadczenia żądanych usług musi również uwzględniać zasadę minimalizacji danych i musi gromadzić wyłącznie dane osobowe niezbędne do świadczenia konkretnych usług płatniczych, o które zwrócił się użytkownik usług płatniczych. Co do zasady, dostęp do danych osobowych powinien być ograniczony do zakresu niezbędnego do świadczenia usług płatniczych. Jak wykazano w rozdziale 2, PSD2 nakłada na dostawców usług płatniczych prowadzących rachunek obowiązek udostępniania informacji o użytkowniku usług płatniczych na wniosek użytkownika usług płatniczych, gdy ten chce skorzystać z usługi inicjowania płatności lub usługi dostępu do informacji o rachunku.

63. W przypadku gdy nie wszystkie dane dotyczące rachunku płatniczego są niezbędne do wykonania umowy, dostawca świadczący usługę dostępu do informacji o rachunku powinien dokonać wyboru odpowiednich kategorii danych przed ich zgromadzeniem. Na przykład kategorie danych, które mogą nie być niezbędne, mogą obejmować tożsamość milczącej strony i charakterystykę transakcji. Ponadto, o ile nie wymaga tego prawo państwa członkowskiego lub prawo Unii, nie ma potrzeby podawania IBAN rachunku bankowego milczącej strony.

64. W tym względzie można rozważyć ewentualne zastosowanie środków technicznych, które umożliwiają dostawcom usług będących osobami trzecimi wypełnianie ich obowiązku dotyczącego dostępu do jedynie tych danych osobowych i pobierania jedynie tych danych osobowych, które są niezbędne do świadczenia ich usług, lub wspierają dostawców w wypełnianiu tego obowiązku, w ramach wdrażania odpowiednich polityk ochrony danych, zgodnie z art. 24 ust. 2 RODO. W tym względzie EROD zaleca stosowanie narzędzi cyfrowych w celu wspierania dostawców świadczących usługę dostępu do informacji o rachunku w wypełnianiu ich obowiązku gromadzenia wyłącznie tych danych osobowych, które są niezbędne do celów, do których są one przetwarzane. Na przykład, gdy dostawca usług nie potrzebuje charakterystyki transakcji (w polu opisu zapisów transakcji) do świadczenia swoich usług, cyfrowe narzędzie wyboru mogłoby funkcjonować jako środek umożliwiający dostawcom usług będącym osobami trzecimi wyłączenie tego pola z ogólnych operacji przetwarzania przez tych dostawców.

> Przykład 2:
>
> HappyPayments, nasz dostawca usług dostępu do informacji o rachunku z przykładu 1, chce zapewnić, aby w ramach jego usług przetwarzane były wyłącznie te dane osobowe dotyczące rachunku płatniczego, którymi są zainteresowani jego użytkownicy. Uzyskanie dostępu do większej ilości danych dotyczących rachunku płatniczego nie byłoby konieczne do świadczenia usługi. W związku z tym umożliwia użytkownikom wybór konkretnych rodzajów informacji, którymi są zainteresowani.
>
> Użytkownik A chce mieć przegląd swoich wydatków z ostatnich dwóch miesięcy. W związku z tym w odniesieniu do swoich dwóch rachunków bankowych prowadzonych przez dwóch różnych dostawców usług płatniczych prowadzących rachunek prosi o podanie informacji o wszystkich transakcjach z ostatnich dwóch miesięcy, ze wskazaniem kwoty transakcji, daty wykonania i nazwy odbiorcy, a następnie zaznacza odpowiednie pola w interfejsie użytkownika HappyPayments.
>
> Następnie HappyPayments rozpoczyna procedurę żądania od odpowiednich dostawców usług płatniczych prowadzących rachunek wyłącznie tych informacji, które odpowiadają polom zaznaczonym przez użytkownika A i dotyczą wyłącznie okresu ostatnich dwóch miesięcy. Informacje, takie jak „tytuł" przelewu lub nawet IBAN, nie są wymagane, ponieważ użytkownik A nie prosił o nie.
>
> Aby umożliwić HappyPayments wywiązanie się z obowiązków w zakresie minimalizacji danych, dostawcy usług płatniczych prowadzący rachunek pozwalają HappyPayments na żądanie określonych pól w danym przedziale czasowym.

65. W tym względzie należy również zauważyć, że zgodnie z PSD2 dostawcy usług płatniczych prowadzący rachunek mogą zapewniać dostęp wyłącznie do informacji o rachunku płatniczym. Na

[34] EROD, Wytyczne 2/2019 w sprawie przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. b) RODO w kontekście świadczenia usług online na rzecz osób, których dane dotyczą, pkt 32.
[35] EROD, Wytyczne 4/2019 dotyczące artykułu 25 Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych, s. 29.

mocy tej dyrektywy nie ma podstawy prawnej do zapewnienia dostępu do danych osobowych zawartych na innych rachunkach, takich jak rachunki oszczędnościowe, hipoteczne lub inwestycyjne. W związku z tym zgodnie z PSD2 należy wdrożyć środki techniczne w celu zapewnienia, aby dostęp był ograniczony do niezbędnych informacji o rachunku płatniczym.

66. Oprócz gromadzenia jak najmniejszej ilości danych dostawca usług musi również wprowadzić ograniczone okresy przechowywania danych. Dane osobowe nie powinny być przechowywane przez dostawcę usług przez okres dłuższy niż jest to niezbędne w związku z celami wskazanymi przez użytkownika usług płatniczych.

67. Jeżeli umowa pomiędzy osobą, której dane dotyczą, a dostawcą świadczącym usługę dostępu do informacji o rachunku wymaga przekazania danych osobowych stronom trzecim, wówczas można przekazać tylko te dane osobowe, które są niezbędne do wykonania umowy. Należy również wyraźnie poinformować osoby, których dane dotyczą, o przekazaniu danych i o tym, jakie dane osobowe mają być przekazane tej stronie trzeciej.

6.3 Bezpieczeństwo

68. EROD podkreśliła już, że naruszenie finansowych danych osobowych „ma wyraźny wpływ na codzienne życie osób, których dane dotyczą", a jako przykład podała ryzyko oszustw płatniczych[36].

69. W przypadku naruszenia danych finansowych osoba, której dane dotyczą, może być narażona na znaczne ryzyko. W zależności od informacji, które wyciekły, osoby, których dane dotyczą, mogą być narażone na ryzyko kradzieży tożsamości, kradzieży środków znajdujących się na ich rachunkach i innych aktywów. Ponadto istnieje możliwość, że ujawnienie danych o transakcjach będzie wiązało się ze znacznym zagrożeniem dla prywatności, ponieważ dane o transakcjach mogą zawierać odniesienia do wszystkich aspektów życia prywatnego osoby, której dane dotyczą. Jednocześnie dane finansowe są oczywiście cenne dla przestępców, a zatem stanowią atrakcyjny cel.

70. Jako administratorzy dostawcy usług płatniczych są zobowiązani do podjęcia odpowiednich środków w celu ochrony danych osobowych osób, których dane dotyczą (art. 24 ust. 1 RODO). Im wyższe ryzyko związane z czynnością przetwarzania realizowaną przez administratora, tym wyższe standardy bezpieczeństwa należy stosować. W związku z tym, że przetwarzanie danych finansowych wiąże się z wieloma poważnymi zagrożeniami, środki bezpieczeństwa powinny być odpowiednio wysokie.

71. Dostawców usług należy objąć wysokimi standardami, w tym mechanizmami silnego uwierzytelniania klienta oraz wysokimi standardami bezpieczeństwa sprzętu technicznego[37]. Ważne są również inne procedury, takie jak weryfikacja podmiotów przetwarzających pod kątem standardów bezpieczeństwa oraz wdrożenie procedur zapobiegających nieuprawnionemu dostępowi.

6.4 Przejrzystość i rozliczalność

72. Przejrzystość i rozliczalność to dwie podstawowe zasady RODO.

73. W odniesieniu do przejrzystości (art. 5 ust. 1 lit. a) RODO) w art. 12 RODO określono, że administratorzy podejmują odpowiednie środki, aby udzielić wszelkich informacji, o których mowa w art. 13 i 14 RODO. Ponadto w artykule tym wymaga się, aby w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie udzielić wszelkich informacji lub prowadzić komunikację w sprawie przetwarzania danych osobowych. Informacji udziela się jasnym i prostym językiem, na piśmie lub „w inny sposób, w tym w stosownych przypadkach – elektronicznie". W Wytycznych w sprawie przejrzystości na podstawie rozporządzenia 2016/679 opracowanych przez Grupę Roboczą Art. 29 i zatwierdzonych przez EROD, przedstawiono konkretne wytyczne dotyczące zgodności z zasadą przejrzystości w środowiskach cyfrowych.

74. Zgodnie z wyżej wspomnianymi wytycznymi w sprawie przejrzystości na podstawie rozporządzenia 2016/679 art. 11 RODO należy interpretować jako sposób egzekwowania rzeczywistej minimalizacji danych pozostający bez uszczerbku dla wykonywania przez osoby, których dane dotyczą, przysługujących im praw, oraz że należy umożliwić wykonywanie praw osoby, której dane dotyczą, przy pomocy dodatkowych informacji dostarczonych przez tę osobę. Mogą zaistnieć sytuacje, w których administrator przetwarza dane osobowe, co nie wymaga identyfikacji osoby, której dane dotyczą (na przykład w przypadku danych spseudonimizowanych). W takich przypadkach istotny może być również art. 11 ust. 1, ponieważ stanowi on, że administrator nie ma obowiązku zachowania, uzyskania ani przetworzenia dodatkowych informacji w celu zidentyfikowania osoby, której dane dotyczą, wyłącznie po to, by zastosować się do RODO.

75. W przypadku usług świadczonych na mocy PSD2 art. 13 RODO ma zastosowanie do danych osobowych zebranych od osoby, której dane dotyczą, a art. 14 ma zastosowanie w przypadku, gdy danych osobowych nie pozyskano od osoby, której dane dotyczą.

76. W szczególności należy poinformować osobę, której dane dotyczą, o okresie, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, o kryteriach ustalania tego okresu, a także, w stosownych przypadkach, o uzasadnionych interesach realizowanych przez administratora lub ewentualną stronę trzecią. Jeżeli przetwarzanie danych odbywa się na podstawie zgody, o której mowa w art. 6 ust. 1 lit. a) RODO, lub wyraźnej zgody, o której mowa w art. 9 ust. 2 lit. a) RODO, należy poinformować osobę, której dane dotyczą, o istnieniu prawa do cofnięcia zgody w dowolnym momencie.

77. Administrator udziela informacji osobie, której dane dotyczą, mając na uwadze konkretne okoliczności przetwarzania danych osobowych. Jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą[38] – co prawdopodobnie będzie miało miejsce w przypadku dostawców świadczących usługę dostępu do informacji o rachunku – informacje muszą zostać udzielone najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą. Jeżeli planuje się ujawnić dane osobowe innemu odbiorcy, informacje muszą zostać udzielone najpóźniej przy ich pierwszym ujawnieniu.

78. W odniesieniu do usług płatniczych online we wspomnianych wytycznych wyjaśniono, że administratorzy mogą przyjąć warstwowe podejście, jeżeli chcą połączyć różne metody w celu zapewnienia przejrzystości. Zaleca się w szczególności, aby korzystano z warstwowych oświadczeń o ochronie prywatności/warstwowych informacji o polityce prywatności w celu odsyłania do różnych kategorii informacji, które należy podać osobie, której dane dotyczą, zamiast wyświetlać na ekranie wszystkie te informacje w formie ciągłego tekstu, aby nie przytłoczyć użytkownika informacjami, a jednocześnie zapewnić skuteczność informacji.

79. We wspomnianych wytycznych wyjaśniono również, że administratorzy mogą postanowić, że zastosują dodatkowe narzędzia w celu przekazania informacji poszczególnym osobom, których dane dotyczą, takie jak pulpity nawigacyjne prywatności. Pulpit nawigacyjny prywatności jest

[36] Grupa Robocza Art. 29, Wytyczne dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko" do celów rozporządzenia 2016/679, WP248 rev.01 - zatwierdzone przez EROD.

[37] Zob. regulacyjny standard techniczny.

[38] Art. 14 ust. 3 lit. b) RODO.

jednym punktem, z którego osoby, których dane dotyczą, mogą przeglądać informacje na temat ochrony prywatności i zarządzać swoimi preferencjami w zakresie prywatności, zezwalając na określone sposoby wykorzystania danych, które ich dotyczą, przez przedmiotowego administratora albo uniemożliwiając takie wykorzystanie[39]. Pulpit nawigacyjny prywatności mógłby zapewnić przegląd dostawców usług będących osobami trzecimi, którzy uzyskali wyraźną zgodę osób, których dane dotyczą, oraz mógłby również oferować odpowiednie informacje na temat charakteru i ilości danych osobowych, do których dostęp uzyskali dostawcy usług będący osobami trzecimi. Dostawca usług płatniczych prowadzący rachunek może co do zasady oferować użytkownikowi możliwość wycofania określonej wyraźnej zgody, o której mowa w PSD2[40], za pośrednictwem przeglądu, co skutkowałoby odmową dostępu do jego rachunków płatniczych jednemu dostawcy usług będącemu osobą trzecią lub większej ich liczbie. Użytkownik może również zwrócić się do dostawcy usług płatniczych prowadzącego rachunek o odmówienie dostępu do jego rachunku płatniczego (rachunków płatniczych) jednemu konkretnemu dostawcy usług będącemu osobą trzecią lub większej ich liczbie[41], ponieważ użytkownik ma prawo do (nie)korzystania z usługi dostępu do informacji o rachunku. Jeżeli w celu udzielenia lub wycofania wyraźnej zgody stosuje się pulpity nawigacyjne prywatności, powinny one być zaprojektowane i stosowane zgodnie z prawem, a w szczególności powinny one zapobiegać tworzeniu przeszkód dla prawa dostawców usług będących osobami trzecimi do świadczenia usług zgodnie z PSD2. W tym względzie i zgodnie z obowiązującymi przepisami PSD2 dostawca usług będący osobą trzecią ma możliwość ponownego uzyskania wyraźnej zgody od użytkownika po jej wycofaniu.

80. Zasady rozliczalności wymagają od administratora ustanowienia odpowiednich środków technicznych i organizacyjnych w celu zapewnienia, aby przetwarzanie odbywało się zgodnie z RODO, w szczególności z głównymi zasadami ochrony danych przewidzianymi w art. 5 ust. 1, a także w celu umożliwienia wykazania, że przetwarzanie jest zgodne z RODO. Środki te powinny uwzględniać charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych, a w razie potrzeby muszą być poddawane przeglądowi i aktualizowane[42].

6.5 Profilowanie

81. Przetwarzanie danych osobowych przez dostawców usług płatniczych może wiązać się z „profilowaniem", o którym mowa w art. 4 pkt 4 RODO. Na przykład dostawcy świadczący usługę dostępu do informacji o rachunku mogą polegać na zautomatyzowanym przetwarzaniu danych osobowych w celu oceny niektórych czynników osobowych osoby fizycznej. W zależności od specyfiki usługi można by ocenić osobistą sytuację finansową osoby, której dane dotyczą. Usługi dostępu do informacji o rachunkach, które mają być świadczone na żądanie użytkowników, mogą obejmować szeroko zakrojoną ocenę danych dotyczących osobistych rachunków płatniczych.

[39] Zgodnie z Wytycznymi Grupy Roboczej Art. 29 w sprawie przejrzystości na podstawie rozporządzenia 2016/679 – zatwierdzonymi przez EROD – pulpity nawigacyjne prywatności są szczególnie przydatne w przypadku korzystania przez osoby, których dane dotyczą, z tej samej usługi na różnych urządzeniach, ponieważ zapewniają im dostęp do ich danych osobowych i kontrolę nad tymi danymi bez względu na sposób korzystania z usługi. Umożliwienie osobom, których dane dotyczą, ręcznego dostosowania ustawień prywatności za pośrednictwem pulpitu nawigacyjnego prywatności może również ułatwić spersonalizowanie oświadczenia o ochronie prywatności / informacji o polityce prywatności poprzez uwzględnienie jedynie tych rodzajów przetwarzania, które mają miejsce w przypadku danej osoby.

[40] Zob. np. „wyraźna zgoda", o której mowa w art. 67 ust. 2 lit. a) drugiej dyrektywy w sprawie usług płatniczych.

[41] Zob. także EBA/OP/2020/10, pkt 45.

[42] Art. 5 ust. 2 i art. 24 RODO.

82. Zachowanie administratora wobec osoby, której dane dotyczą, musi być również przejrzyste w kwestii istnienia zautomatyzowanego podejmowania decyzji, w tym profilowania. W tych przypadkach administrator musi przedstawić istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą (art. 13 ust. 2 lit. f) i art. 14 ust. 2 lit. g) oraz motyw 60)[43]. Podobnie, zgodnie z art. 15 RODO, osoba, której dane dotyczą, ma prawo zażądać od administratora informacji o istnieniu zautomatyzowanego podejmowania decyzji, w tym o profilowaniu, informacji o zasadach ich podejmowania i konsekwencjach dla osoby, której dane dotyczą, oraz ma prawo uzyskać takie informacje, a także, w pewnych okolicznościach, ma prawo do sprzeciwu wobec profilowania, niezależnie od tego, czy ma miejsce wyłącznie zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach w oparciu o profilowanie[44].

83. Ponadto w tym kontekście istotne jest również prawo osoby, której dane dotyczą, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa, zgodnie z art. 22 RODO. Norma ta obejmuje również, w pewnych okolicznościach, konieczność wdrożenia przez administratorów odpowiednich środków ochrony praw osób, których dane dotyczą, takich jak szczegółowe informacje dla osób, których dane dotyczą, prawo do uzyskania interwencji ludzkiej w procesie podejmowania decyzji oraz do wyrażenia własnego stanowiska i do zakwestionowania tej decyzji. Jak stwierdzono również w motywie 71 RODO, oznacza to m.in., że osoby, których dane dotyczą, mają prawo nie podlegać decyzji, takiej jak automatyczne odrzucenie elektronicznego wniosku kredytowego bez interwencji ludzkiej[45].

84. Zautomatyzowane podejmowanie decyzji, w tym profilowanie, w toku którego dochodzi do przetwarzania szczególnych kategorii danych osobowych, uznaje się za dopuszczalne wyłącznie w przypadku łącznego spełnienia warunków określonych w art. 22 ust. 4 RODO:

- istnieje możliwość zastosowania odstępstwa, o którym mowa w art. 22 ust. 2;
- oraz zastosowanie ma art. 9 ust. 2 lit. a) lub g) RODO. W obydwu przypadkach administrator ustanawia odpowiednie środki zapewniające osobie, której dane dotyczą, poszanowanie jej praw i wolności oraz prawnie uzasadnionych interesów[46].

85. Należy również przestrzegać wymogów dotyczących dalszego przetwarzania, jak określono w niniejszych wytycznych. Wyjaśnienia i instrukcje dotyczące zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania podane przez Grupę Roboczą Art. 29 w zatwierdzonych przez EROD Wytycznych w sprawie zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania do celów rozporządzenia 2016/679, są w pełni istotne w kontekście usług płatniczych i dlatego należy je należycie rozważyć.

W imieniu Europejskiej Rady Ochrony Danych

[43] Wytyczne w sprawie przejrzystości na podstawie rozporządzenia 2016/679, GR 260 rev.01 – zatwierdzone przez EROD.

[44] Wytyczne Grupy Roboczej Art. 29 w sprawie zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania do celów rozporządzenia 2016/679, WP251rev.01.

[45] Motyw 71 RODO.

[46] Wytyczne Grupy Roboczej Art. 29, w sprawie zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania do celów rozporządzenia 2016/679, WP251rev.01, s. 24.

Przewodnicząca

(Andrea Jelinek)



Wytyczne 05/2020 dotyczące zgody na mocy rozporządzenia 2016/679

Wersja 1.1

Przyjęta dnia 4 maja 2020 r.

Translations proofread by EDPB Members.

This language version has not been proofread.

Historia wersji

Wersja 1.1	13 maja 2020 r.	Poprawki formatowania
Wersja 1.0	4 maja 2020 r.	Przyjęcie wytycznych

Spis treści

0 Wprowadzenie ... 4
1 Wprowadzenie ... 4
2 Pojęcie zgody zawarte w art. 4 pkt 11 RODO ... 6
3 Elementy ważnej zgody ... 7
3.1 Dobrowolna / dobrowolnie wyrażona ... 7
3.1.1 Brak równowagi sił ... 8
3.1.2 Warunkowość ... 10
3.1.3 Szczegółowość ... 13
3.1.4 Niekorzystne konsekwencje ... 13
3.2 Konkretność ... 14
3.3 Świadoma ... 16
3.3.1 Minimalne wymogi dotyczące treści, aby zgoda była „świadoma" ... 16
3.3.2 W jaki sposób należy przekazywać informacje? ... 17
3.4 Jednoznaczne okazanie woli ... 19
4 Uzyskanie wyraźnej zgody ... 22
5 Dodatkowe warunki uzyskania ważnej zgody ... 24
5.1 Wykazanie zgody ... 24
5.2 Wycofanie zgody ... 25
6 Zależność między zgodą a innymi zgodnymi z prawem podstawami, o których mowa w art. 6 RODO ... 27
7 Szczególnie istotne obszary w RODO ... 28
7.1 Dzieci (art. 8) ... 28
7.1.1 Usługi społeczeństwa informacyjnego ... 29
7.1.2 Usługi oferowane bezpośrednio dziecku ... 29
7.1.3 Wiek ... 30
7.1.4 Zgoda udzielana przez dzieci i władza rodzicielska ... 30
7.2 Badania naukowe ... 33
7.3 Prawa osób, których dane dotyczą ... 35
8 Zgoda uzyskana na mocy dyrektywy 95/46/WE ... 35

Europejska Rada Ochrony Danych,

uwzględniając art. 70 ust. 1 lit. e) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (zwanego dalej „RODO"),

uwzględniając Porozumienie EOG, w szczególności załącznik XI i protokół 37 do tego Porozumienia, zmienione decyzją Wspólnego Komitetu EOG nr 154/2018 z dnia 6 lipca 2018 r.[1],

uwzględniając art. 12 i 22 swojego regulaminu wewnętrznego,

uwzględniając wytyczne Grupy Roboczej Art. 29 dotyczące zgody na mocy rozporządzenia 2016/679, WP259 rev. 01,

PRZYJĘŁA NASTĘPUJĄCE WYTYCZNE:

0 WPROWADZENIE

W dniu 10 kwietnia 2018 r. Grupa Robocza Art. 29 (GR29) przyjęła swoje wytyczne dotyczące zgody na mocy rozporządzenia 2016/679 (WP259.01), które Europejska Rada Ochrony Danych (zwana dalej „EROD") zatwierdziła na swoim pierwszym posiedzeniu plenarnym. Niniejszy dokument jest wersją tych wytycznych z niewielkim zmianami służącymi aktualizacji. Wszelkie odniesienia do wytycznych GR29 dotyczących zgody (WP259 rev. 01) należy z chwilą obecną rozumieć jako odniesienia do niniejszych wytycznych.

EROD zauważył, że potrzebne są dalsze wyjaśnienia, dotyczące konkretnie dwóch kwestii:

1 ważności zgody udzielonej przez osobę, której dane dotyczą, w reakcji na tzw. *cookie wall*;
2 przykładu nr 16 dotyczącego przewijania stron w dół i zgody.

Punkty dotyczące tych dwóch kwestii zostały poprawione i zaktualizowane, natomiast do reszty dokumentu wprowadzono wyłącznie zmiany redakcyjne. Wprowadzone poprawki obejmują:

- sekcję dotyczącą warunkowości (pkt 38–41);
- sekcję dotyczącą jednoznacznego okazania woli (pkt 86).

1 WPROWADZENIE

1. Niniejsze wytyczne zawierają szczegółową analizę pojęcia zgody zastosowanego w rozporządzeniu 2016/679, tj. w ogólnym rozporządzeniu o ochronie danych (zwanym dalej „RODO"). Pojęcie zgody stosowane dotychczas w dyrektywie o ochronie danych (zwanej dalej „dyrektywą 95/46/WE") oraz w dyrektywie o prywatności i łączności elektronicznej ewoluowało. W RODO jeszcze bardziej sprecyzowano i uszczegółowiono wymogi dotyczące uzyskania ważnej zgody oraz wykazania jej wyrażenia. W niniejszych wytycznych skoncentrowano się na tych zmianach i sformułowano praktyczne wskazówki w celu zapewnienia zgodności z RODO, opierając się na opinii 15/2011 Grupy Roboczej Art. 29 w sprawie definicji zgody. Na administratorach danych spoczywa obowiązek wprowadzania innowacji w celu znalezienia nowych rozwiązań, które funkcjonują w ramach prawnych i lepiej wspierają ochronę danych osobowych oraz interesy osób, których dane dotyczą.

2. Zgoda jest jedną z sześciu zgodnych z prawem podstaw przetwarzania danych osobowych wymienionych w art. 6 RODO[2]. Rozpoczynając działalność, która wiąże się z przetwarzaniem danych osobowych, administrator musi zawsze poświęcić pewien czas na zastanowienie się, jaka byłaby odpowiednia zgodna z prawem podstawa planowanego przetwarzania.

3. Co do zasady zgoda może być właściwą, zgodną z prawem podstawą wyłącznie wówczas, gdy osobie, której dane dotyczą, zapewnia się kontrolę oraz rzeczywistą możliwość wyboru w odniesieniu do przyjęcia lub odrzucenia zaoferowanych warunków lub odrzucenia ich bez niekorzystnych konsekwencji. Zwracając się o zgodę, administrator ma obowiązek oceny, czy spełni wszystkie wymogi uzyskania ważnej zgody. Zgoda uzyskana w pełnej zgodności z RODO jest narzędziem zapewniającym osobom, których dane dotyczą, kontrolę nad tym, czy dotyczące ich dane osobowe będą przetwarzane. W braku zgodności zgody z RODO kontrola ze strony osoby, której dane dotyczą, staje się złudna, a zgoda będzie nieważną podstawą przetwarzania, co spowoduje niezgodność z prawem czynności przetwarzania[3].

4. Istniejące opinie Grupy Roboczej Art. 29 w sprawie zgody[4] nadal mają zastosowanie, jeżeli są zgodne z nowymi ramami prawnymi, ponieważ w RODO skodyfikowano istniejące wytyczne GR29 i ogólne dobre praktyki oraz większość najważniejszych elementów zgody pozostaje jednakowa na mocy RODO. W niniejszym dokumencie EROD rozszerza i uzupełnia zatem wcześniejsze opinie Grupy Roboczej Art. 29 dotyczące określonych zagadnień, które zawierają odniesienie do zgody na mocy dyrektywy 95/46/WE, nie zastępując tych opinii.

5. Jak GR29 stwierdziła w swojej opinii 15/2011 w sprawie definicji zgody, zwracanie się do osób o wyrażenie zgody na czynność przetwarzania danych powinno podlegać rygorystycznym wymogom, ponieważ dotyczy praw podstawowych osób, których dane dotyczą, a administrator pragnie przeprowadzić operację przetwarzania, która byłaby niezgodna z prawem bez zgody osoby, której dane dotyczą[5]. Kluczową rolę zgody podkreślono w art. 7 i 8 Karty praw podstawowych Unii Europejskiej. Ponadto również uzyskanie zgody nie zwalnia administratora z obowiązków przestrzegania zasad przetwarzania zawartych w RODO, w szczególności w art. 5 RODO, w odniesieniu do rzetelności,

[1] Odniesienia do „państw członkowskich" zawarte w niniejszym dokumencie należy rozumieć jako odniesienia do „państw członkowskich EOG".

[2] Art. 9 RODO zawiera wykaz możliwych wyjątków od zakazu przetwarzania szczególnych kategorii danych. Jeden z wymienionych wyjątków dotyczy sytuacji, w której osoba, której dane dotyczą, udzieli wyraźnej zgody na wykorzystanie tych danych.

[3] Zob. także opinia Grupy Roboczej Art. 29 15/2011 w sprawie definicji zgody (WP 187), s. 6–8, lub opinia 06/2014 w sprawie pojęcia uzasadnionych interesów administratora danych zawartego w art. 7 dyrektywy 95/46/WE (WP 217), s. 9, 10, 13 i 14.

[4] W szczególności opinia 15/2011 w sprawie definicji zgody (WP 187).

[5] Opinia 15/2011, strona dotycząca definicji zgody (WP 187), s. 8.

konieczności i proporcjonalności oraz jakości danych, ani w żaden sposób nie zmniejsza zakresu tych obowiązków. Nawet gdyby osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie danych osobowych, nie uczyniłoby to legalnym gromadzenia danych, które nie są konieczne w związku z określonym celem przetwarzania, i byłoby ono zasadniczo nieuczciwe[6].

6. Jednocześnie EROD jest świadom przeglądu dyrektywy o prywatności i łączności elektronicznej (2002/58/WE). Pojęcie zgody w projekcie rozporządzenia w sprawie prywatności i łączności elektronicznej pozostaje powiązane z pojęciem zgody w RODO[7]. Organizacje prawdopodobnie będą potrzebowały zgody zgodnie z instrumentem dotyczącym prywatności i łączności elektronicznej w odniesieniu do większości internetowych wiadomości marketingowych lub połączeń marketingowych oraz internetowych metod śledzenia, w tym za pośrednictwem plików cookie, aplikacji lub innego oprogramowania. EROD przedstawił już prawodawcy Unii zalecenia i wytyczne w zakresie wniosku dotyczącego rozporządzenia w sprawie prywatności i łączności elektronicznej[8].

7. W odniesieniu do istniejącej dyrektywy o prywatności i łączności elektronicznej EROD zauważa, że odesłania do uchylonej dyrektywy 95/46/WE należy traktować jako odesłania do RODO[9]. Zasada ta ma również zastosowanie do odniesień do zgody zawartych w obowiązującej dyrektywie 2002/58/WE, ponieważ rozporządzenie w sprawie prywatności i łączności elektronicznej nie wejdzie (jeszcze) w życie od dnia 25 maja 2018 r. Zgodnie z art. 95 RODO nie nakłada się dodatkowych obowiązków na osoby fizyczne ani prawne co do przetwarzania w związku ze świadczeniem ogólnodostępnych usług łączności elektronicznej w publicznych sieciach łączności w Unii, o ile w dyrektywie o prywatności i łączności elektronicznej podmioty te podlegają szczegółowym obowiązkom mającym ten sam cel. EROD zauważa, że wymogów uzyskania zgody określonych w RODO nie uznaje się za „dodatkowy obowiązek", lecz raczej za warunki wstępne zgodnego z prawem przetwarzania. Określone w RODO przesłanki uzyskania ważnej zgody mają zatem zastosowanie w sytuacjach objętych zakresem stosowania dyrektywy o prywatności i łączności elektronicznej.

2 POJĘCIE ZGODY ZAWARTE W ART. 4 PKT 11 RODO

8. W art. 4 pkt 11 RODO zdefiniowano zgodę jako: „dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych".

9. Podstawowa koncepcja zgody pozostaje podobna do koncepcji zawartej w dyrektywie 95/46/WE, przy czym zgoda stanowi jedną ze zgodnych z prawem podstaw, na których musi się opierać przetwarzanie danych osobowych, zgodnie z art. 6 RODO[10]. Oprócz zmienionej definicji zawartej w art. 4 pkt 11 RODO zawiera dodatkowe wskazówki w art. 7 oraz w motywach 32, 33, 42 i 43 dotyczące sposobu działania administratora w celu spełnienia głównych elementów wymogu uzyskania zgody.

10. Ponadto uwzględnienie przepisów szczegółowych i motywów dotyczących wycofania zgody potwierdza, że wyrażenie zgody powinno być decyzją odwracalną i że osobie, której dane dotyczą, przysługuje pewien zakres kontroli.

3 ELEMENTY WAŻNEJ ZGODY

11. Art. 4 pkt 11 RODO stanowi, że zgoda osoby, której dane dotyczą, oznacza:

    - dobrowolne,
    - konkretne,
    - świadome
    - i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

12. W poniższych sekcjach przeanalizowano, w jakim zakresie brzmienie art. 4 pkt 11 zobowiązuje administratorów do zmiany zapytań o zgodę / formularzy wyrażenia zgody, aby zapewnić zgodność z RODO[11].

3.1 Dobrowolna / dobrowolnie wyrażona[12]

13. Przymiot „dobrowolności" zakłada rzeczywistą możliwość dokonania wyboru przez osoby, których dane dotyczą, oraz sprawowania przez nie kontroli. Co do zasady RODO stanowi, że jeżeli osobie, której dane dotyczą, nie przysługuje rzeczywista możliwość wyboru, czuje się ona zmuszona do wyrażenia zgody lub poniesie negatywne konsekwencje w przypadku jej niewyrażenia, zgoda będzie nieważna[13].

---

[6] Zob. także opinia 15/2011 w sprawie definicji zgody (WP 187) oraz art. 5 RODO.

[7] Zgodnie z art. 9 proponowanego rozporządzenia w sprawie prywatności i łączności elektronicznej zastosowanie mają definicja i warunki zgody przewidziane w art. 4 pkt 11 i art. 7 RODO.

[8] Zob. oświadczenie EROD dotyczące prywatności i łączności elektronicznej z 25.5.2018 i oświadczenie EROD 3/2019 w sprawie rozporządzenia o prywatności i łączności elektronicznej.

[9] Zob. art. 94 RODO.

[10] Zgodę zdefiniowano w dyrektywie 95/46/WE jako „konkretne i świadome, dobrowolne wskazanie przez osobę, której dane dotyczą na to, że wyraża przyzwolenie na przetwarzanie odnoszących się do niej danych osobowych", przy czym zgoda ta musi być „jednoznacznie wyrażona", aby zapewnić legalność przetwarzania danych osobowych (art. 7 lit. a) dyrektywy 95/46/WE). Zob. opinia GR29 15/2011 w sprawie definicji zgody (WP 187), aby zapoznać się z przykładami stosowności zgody jako podstawy zgodnej z prawem. W opinii tej GR29 przedstawiła wytyczne w celu dokonania rozróżnienia między przypadkami, w których zgoda stanowi właściwą, zgodną z prawem podstawę, a przypadkami, w których wystarczające jest powołanie się na przesłankę uzasadnionego interesu (ewentualnie z możliwością wyrażenia sprzeciwu) lub zalecane byłoby nawiązanie stosunku umownego. Zob. także opinia GR29 06/2014, pkt III.1.2, s. 14 i nast. Wyraźna zgoda stanowi również jeden z wyjątków od zakazu przetwarzania szczególnych kategorii danych: Zob. art. 9 RODO.

[11] Aby uzyskać wskazówki dotyczące bieżących czynności przetwarzania opartych na zgodzie na mocy dyrektywy 95/46, zob. rozdział 7 niniejszego dokumentu oraz motyw 171 RODO.

[12] W szeregu opinii Grupa Robocza Art. 29 zbadała granice zgody w sytuacjach, w których zgoda nie może być dobrowolnie wyrażona. Dokumenty te obejmują w szczególności: opinię 15/2011 w sprawie definicji zgody (WP 187), dokument roboczy w sprawie przetwarzania danych osobowych dotyczących zdrowia w elektronicznej dokumentacji medycznej (WP 131), opinię 8/2001 w sprawie przetwarzanie danych osobowych w związku z zatrudnieniem (WP 48) oraz drugą opinię 4/2009 dotyczącą przetwarzania danych przez Światową Agencję Antydopingową (WADA) (międzynarodowy standard ochrony prywatności i danych osobowych), odpowiednich przepisów kodeksu WADA oraz innych kwestii dotyczących prywatności w kontekście zwalczania dopingu w sporcie przez WADA i inne (krajowe) organizacje antydopingowe (WP 162).

[13] Zob. opinia 15/2011 w sprawie definicji zgody (WP 187), s. 12.

Jeżeli wyrażenie zgody stanowi nieodłączną i niepodlegającą negocjacji część warunków, uznaje się, że nie jest ona dobrowolna. W związku z tym wyrażenie zgody nie zostanie uznane za dobrowolne, jeżeli osoba, której dane dotyczą, nie może odmówić ani wycofać zgody bez niekorzystnych konsekwencji[14]. Pojęcie braku równowagi między administratorem a osobą, której dane dotyczą, również uwzględniono w RODO.

14. Podczas oceny, czy zgodę wyrażono dobrowolnie, należy również uwzględnić szczególną sytuację, w której od wyrażenia zgody uzależnione jest wykonanie umowy lub świadczenie usługi, jak opisano w art. 7 ust. 4. Art. 7 ust. 4 ma charakter katalogu otwartego dzięki zastosowaniu w nim wyrażenia „między innymi", które oznacza, że istnieje również szereg innych sytuacji, które mogą zostać objęte zakresem stosowania tego przepisu. Co do zasady wszelki element niewłaściwej presji lub niewłaściwego wpływu na osobę, której dane dotyczą (mogący się przejawiać na wiele różnych sposobów), uniemożliwiający osobie, której dane dotyczą, swobodne okazanie woli, spowoduje nieważność zgody.

15. Przykład 1: Aplikacja mobilna do edytowania zdjęć prosi użytkowników o aktywowanie lokalizacji GPS w celu rozpoczęcia korzystania z jej usług. Aplikacja informuje również użytkowników, że będzie wykorzystywała zgromadzone dane do celów reklamy behawioralnej. Ani geolokalizacja, ani internetowa reklama behawioralna nie są konieczne do świadczenia usługi edytowania zdjęć i wykraczają one poza świadczenie podstawowej usługi. Ponieważ użytkownicy nie mogą korzystać z aplikacji bez wyrażenia zgody na te usługi, nie można uznać zgody za wyrażoną dobrowolnie.

3.1.1 Brak równowagi sił

16. Motyw 43[15] wyraźnie stanowi, że jest mało prawdopodobne, by **organy publiczne** mogły opierać się na zgodzie na przetwarzanie, ponieważ jeżeli administratorem jest organ publiczny, często istnieje wyraźny brak równowagi w stosunkach między administratorem a osobą, której dane dotyczą. W większości przypadków nie ulega również wątpliwości, że osoba, której dane dotyczą, nie będzie miała realnej alternatywy wobec zaakceptowania (warunków) przetwarzania zaproponowanych przez tego administratora. EROD twierdzi, że istnieją inne zgodne z prawem podstawy, które są co do zasady właściwsze w przypadku działalności organów publicznych[16].

17. Bez uszczerbku dla tych ogólnych rozważań możliwość wykorzystania zgody jako zgodnej z prawem podstawy przetwarzania danych przez organy publiczne nie jest całkowicie wykluczona zgodnie z ramami prawnymi RODO. Poniższe przykłady pokazują, że wykorzystanie zgody może być właściwe w pewnych okolicznościach.

18. Przykład 2: Gmina planuje przeprowadzenie robót konserwacyjnych na drogach. Ponieważ roboty drogowe mogą powodować długotrwałe utrudnienia w ruchu, gmina oferuje mieszkańcom możliwość zapisania się na listę dystrybucyjną, aby otrzymywać aktualne informacje na temat postępu robót i oczekiwanych opóźnień. Gmina wyjaśnia, że zapisanie się na listę nie jest obowiązkowe, i zwraca się o wyrażenie zgody na wykorzystanie adresów e-mailowych (wyłącznie) w tym celu. Mieszkańcy, którzy nie wyrażą zgody, nie stracą możliwości korzystania z jakiejkolwiek podstawowej usługi gminy ani możliwości wykonania jakiegokolwiek przysługującego im prawa, a zatem mogą dobrowolnie wyrazić zgodę lub odmówić wyrażenia zgody na wykorzystanie tych danych. Wszystkie informacje na temat robót drogowych będą również dostępne na stronie internetowej gminy.

19. Przykład 3: Osoba fizyczna będąca właścicielem gruntu musi uzyskać określone zezwolenia zarówno od gminy, jak i od jednostki samorządu terytorialnego wyższego szczebla, której podlega gmina. Obydwa organy publiczne wymagają dostarczenia tych samych informacji w celu wydania zezwolenia, ale nie mają wzajemnego dostępu do swoich baz danych. Obydwa organy zwracają się zatem o te same informacje dotyczące gruntu, a jego właściciela przekazuje swoje dane obydwu tym instytucjom. Gmina oraz jednostka samorządu terytorialnego wyższego szczebla zwracają się do właścicielki o wyrażenie zgody na połączenie akt, aby uniknąć powielania procedur i korespondencji. Obydwa organy publiczne zapewniają, że jest to nieobowiązkowe i że wnioski o zezwolenie zostaną rozpatrzone osobno, jeżeli nie wyrazi ona zgody na połączenie danych. Wyrażenie przez właścicielkę zgody na połączenie akt przez organy można uznać za dobrowolne.

20. Przykład 4: Szkoła publiczna zwraca się do uczniów o wyrażenie zgody na wykorzystanie ich zdjęć w czasopiśmie szkolnym wydawanym w formie papierowej. W tych sytuacjach uczniowie będą mieli faktyczny wybór, jeśli chodzi o wyrażenie zgody, dopóki nie zostanie im odmówiony dostęp do kształcenia lub usług i dopóki będą mogli odmówić wykorzystania tych zdjęć bez żadnych niekorzystnych konsekwencji[17].

21. Brak równowagi sił występuje również w związku z **zatrudnieniem**[18]. Biorąc pod uwagę zależność charakteryzującą stosunek między pracodawcą a pracownikiem, nie jest prawdopodobne, by osoba, której dane dotyczą, mogła odmówić pracodawcy zgody na przetwarzanie danych, nie doświadczając obaw lub faktycznego ryzyka poniesienia niekorzystnych konsekwencji w wyniku odmowy. Nie jest prawdopodobne, by pracownik mógł swobodnie odpowiedzieć na wniosek pracodawcy o wyrażenie zgody na przykład na uruchomienie systemów monitorowania, takich jak nadzór kamer w miejscu pracy, lub wypełnienie formularzy oceny, nie odczuwając żadnej presji na wyrażenie zgody[19]. EROD uznaje zatem, że w przypadku pracodawców problematyczne jest przetwarzanie danych osobowych obecnych lub przyszłych pracowników w oparciu o ich zgodę, ponieważ jest mało prawdopodobne, by została ona wyrażona dobrowolnie. W odniesieniu do większości przypadków przetwarzania danych w miejscu pracy zgodną z prawem podstawą nie może i nie powinna być zgoda pracowników (art. 6 ust. 1 lit. a)) ze względu na charakter stosunków między pracodawcą a pracownikiem[20].

[14] Zob. motywy 42, 43 RODO oraz opinia GR29 15/2011 w sprawie definicji zgody przyjęta dnia 13 lipca 2011 r. (WP 187), s. 12.

[15] Motyw 43 RODO stanowi: „Aby zapewnić dobrowolność, zgoda nie powinna stanowić ważnej podstawy prawnej przetwarzania danych osobowych w szczególnej sytuacji, w której istnieje wyraźny brak równowagi między osobą, której dane dotyczą, a administratorem, w szczególności gdy administrator jest organem publicznym i dlatego jest mało prawdopodobne, by w tej konkretnej sytuacji zgodę wyrażono dobrowolnie we wszystkich przypadkach (...)".

[16] Zob. art. 6 RODO, w szczególności jego ust. 1 lit. c) oraz ust. 1 lit. e).

[17] Do celów niniejszego przykładu szkoła publiczna oznacza szkołę sfinansowaną ze środków publicznych lub dowolną placówkę edukacyjną zakwalifikowaną jako organ lub podmiot publiczny na mocy prawa krajowego.

[18] Zob. także art. 88 RODO, w którym podkreślono potrzebę ochrony szczególnych interesów pracowników oraz stworzono możliwość ustanowienia wyjątków w przepisach państwa członkowskiego. Zob. także motyw 155.

[19] Zob. opinia 15/2011 w sprawie definicji zgody (WP 187), s. 12–14, opinia 8/2001 w sprawie przetwarzania danych osobowych w związku z zatrudnieniem (WP 48), rozdział 10, dokument roboczy w sprawie nadzoru komunikacji elektronicznej w miejscu pracy (WP 55), pkt 4.2, oraz opinia 2/2017 na temat przetwarzania danych w miejscu pracy (WP 249), pkt 6.2.

[20] Zob. opinia 2/2017 na temat przetwarzania danych w miejscu pracy, s. 6–7.

22. Nie oznacza to jednak, że pracodawcy nigdy nie mogą powoływać się na zgodę jako zgodną z prawem podstawę przetwarzania. Mogą się zdarzyć sytuacje, w których pracodawca ma możliwość wykazania, że zgody faktycznie udzielono dobrowolnie. Biorąc pod uwagę brak równowagi sił między pracodawcą a jego pracownikami, pracownicy mogą wyrazić dobrowolną zgodę wyłącznie w wyjątkowych okolicznościach, w których fakt wyrażenia lub niewyrażenia przez nich zgody nie pociąga za sobą żadnych negatywnych konsekwencji[21].

23. Przykład 5: Ekipa filmowa ma zamiar nagrywać w określonej części biura. Pracodawca zwraca się do wszystkich pracowników siedzących w tej części o wyrażenie zgody na filmowanie, ponieważ ich wizerunek może się pojawić na drugim planie filmu. Osoby, które nie chcą być filmowane, nie ponoszą żadnych negatywnych konsekwencji, lecz na czas filmowania otrzymują w zamian takie same biurka w innym miejscu w budynku.

24. Brak równowagi sił nie ogranicza się do organów publicznych i pracodawców – może on zaistnieć również w innych sytuacjach. Jak podkreśliła GR29 w szeregu opinii, zgoda może być ważna wyłącznie wówczas, gdy osoba, której dane dotyczą, ma możliwość dokonania rzeczywistego wyboru i nie zachodzi ryzyko wprowadzenia w błąd, zastraszenia, przymusu lub znaczących negatywnych konsekwencji (np. znaczących kosztów dodatkowych), jeżeli nie wyrazi zgody. Zgoda nie będzie dobrowolna wówczas, gdy pojawi się jakikolwiek element przymusi, presji lub braku możliwości swobodnego okazania woli.

3.1.2 Warunkowość

25. Podczas oceny, czy zgodę wyrażono dobrowolnie, istotną rolę odgrywa art. 7 ust. 4 RODO[22].

26. Art. 7 ust. 4 RODO stanowi, że za wysoce niepożądaną uznaje się między innymi sytuację łączenia zgody z akceptacją warunków lub uzależniania wykonania umowy lub świadczenia usługi od uwzględnienia wniosku o wyrażenie zgody na przetwarzanie danych osobowych, które nie jest konieczne w celu wykonania umowy lub świadczenia usługi. Jeżeli zgodę wyrażono w takiej sytuacji, uznaje się, że nie była ona dobrowolna (motyw 43). Art. 7 ust. 4 dąży do zapewnienia, by cel przetwarzania danych osobowych nie był ukryty ani połączony z wykonaniem umowy lub świadczeniem usługi, w odniesieniu do których odnośne dane osobowe nie są konieczne. Tym samym RODO zapewnia, by przetwarzanie danych osobowych, którego dotyczy wniosek o wyrażenie zgody, nie nosiło bezpośrednich ani pośrednich znamion świadczenia wzajemnego związanego z wykonaniem umowy. Nie można łączyć obydwu tych legalnych podstaw zgodnego z prawem przetwarzania danych osobowych, tj. zgody i umowy, ani zacierać różnic między nimi.

27. Obowiązek wyrażenia zgody na wykorzystanie danych osobowych w sposób wykraczający poza niezbędne minimum ogranicza przysługującą osobie, której dane dotyczą, możliwość wyboru i uniemożliwia wyrażenie dobrowolnej zgody. Ponieważ celem prawa w dziedzinie ochrony danych jest ochrona praw podstawowych, kontrola osoby fizycznej nad jej danymi osobowymi jest kluczowa, przy

[21] Zob. także opinia 2/2017 na temat przetwarzania danych w miejscu pracy (WP 249), pkt 6.2.

[22] Art. 7 ust. 4 RODO: „Oceniając, czy zgodę wyrażono dobrowolnie, w jak największym stopniu uwzględnia się, czy między innymi od zgody na przetwarzanie danych nie jest uzależnione wykonanie umowy, w tym świadczenie usługi, jeśli przetwarzanie danych osobowych nie jest niezbędne do wykonania tej umowy". Zob. także motyw 43 RODO, który stanowi: „(...) Zgody nie uważa się za dobrowolną, jeżeli nie można jej wyrazić z osobna na różne operacje przetwarzania danych osobowych, mimo że w danym przypadku byłoby to stosowne, lub jeżeli od zgody uzależnione jest wykonanie umowy – w tym świadczenie usługi – mimo że do jej wykonania zgoda nie jest niezbędna".

czym istnieje silne domniemanie, że zgody na przetwarzanie danych osobowych, które nie jest konieczne, nie można postrzegać jako obowiązkowego świadczenia w zamian za wykonanie umowy lub świadczenie usługi.

28. W związku z powyższym w każdym przypadku, w którym wniosek o wyrażenie zgody jest związany z wykonaniem umowy przez administratora, osoba, której dane dotyczą i która nie chce udostępnić swoich danych osobowych w celu ich przetwarzania przez administratora, ponosi ryzyko odmowy świadczenia usług, o które się zwróciła.

29. Aby ocenić, czy w danej sytuacji doszło do powiązania zgody z wykonaniem umowy lub do uzależnienia wykonania umowy od wyrażenia zgody, istotne jest ustalenie zakresu umowy oraz danych, jakie byłyby niezbędne do jej wykonania.

30. Zgodnie z opinią 06/2014 wydaną przez GR29 należy stosować wykładnię zawężającą wyrażenia „niezbędne do wykonania umowy". Przetwarzanie musi być niezbędne do wykonania umowy z każdą konkretną osobą, której dane dotyczą. Może to obejmować na przykład przetwarzanie adresu osoby, której dane dotyczą, żeby można było dostarczyć towary zakupione przez nią w internecie, lub przetwarzanie danych karty kredytowej w celu ułatwienia płatności. W kontekście zatrudnienia podstawa ta może przykładowo umożliwiać przetwarzanie informacji o wynagrodzeniu i danych rachunku bankowego, żeby można było wypłacić wynagrodzenie[23]. Musi istnieć bezpośredni i obiektywny związek między przetwarzaniem danych a celem wykonania umowy.

31. Jeżeli administrator zamierza przetwarzać dane osobowe, które są faktycznie niezbędne do wykonania umowy, zgoda nie jest właściwą, zgodną z prawem podstawą[24].

32. Art. 7 ust. 4 ma zastosowanie wyłącznie wówczas, gdy wnioskowane dane **nie** są niezbędne do wykonania umowy (w tym świadczenia usługi), lecz jej wykonanie uzależniono od uzyskania tych danych w oparciu o zgodę. Jeżeli natomiast przetwarzanie **jest** niezbędne do wykonania umowy (w tym świadczenia usługi), art. 7 ust. 4 nie ma zastosowania.

33. Przykład 6: Bank prosi klientów o zgodę na wykorzystywanie przez osoby trzecie ich danych płatniczych do celów marketingu bezpośredniego. Tego rodzaju czynność przetwarzania nie jest niezbędna do wykonania umowy z klientem i świadczenia zwykłych usług w zakresie rachunków bankowych. Jeżeli niewyrażenie przez klienta zgody na to przetwarzanie doprowadziłoby do odmowy świadczenia usług bankowych, zamknięcia rachunku bankowego lub – w zależności od przypadku – zwiększenia opłaty, nie można uznać zgody za dobrowolną.

34. Decyzja prawodawcy o podkreśleniu m.in. warunkowości jako domniemania braku dobrowolności zgody, pokazuje, że wystąpienie warunkowości należy dokładnie zbadać. Wyrażenie „w jak największym stopniu" zastosowane w art. 7 ust. 4 sugeruje, że administrator powinien zachować szczególną ostrożność, jeżeli umowa (która obejmuje świadczenie usługi) zawiera wniosek o wyrażenie zgody na przetwarzanie danych osobowych.

[23] Aby uzyskać więcej informacji i zapoznać się z przykładami, zob. opinia 06/2014 w sprawie pojęcia uzasadnionych interesów administratora danych zawartego w art. 7 dyrektywy 95/46/WE (WP 217) przyjęta przez GR29 dnia 9 kwietnia 2014 r., s. 16–17.

[24] W takiej sytuacji właściwą, zgodną z prawem podstawą mogłaby być podstawa określona w art. 6 ust. 1 lit. b) (umowa).

35. Ponieważ art. 7 ust. 4 nie został sformułowany w sposób bezwzględny, może istnieć bardzo ograniczona liczba przypadków, w których taka warunkowość nie spowodowałaby nieważności zgody. Zastosowanie terminu „uważa się" w motywie 43 wyraźnie wskazuje jednak, że jest to możliwe wyłącznie w wyjątkowych przypadkach.

36. W każdym przypadku ciężar dowodu zgodnie z art. 7 ust. 4 spoczywa na administratorze[25]. Ten przepis szczegółowy odzwierciedla ogólną zasadę rozliczalności, która przewija się w całym RODO. Jeżeli jednak art. 7 ust. 4 ma zastosowanie, administratorowi będzie trudniej udowodnić, że osoba, której dane dotyczą, udzieliła dobrowolnej zgody[26].

37. Administrator mógłby argumentować, że jego organizacja zapewnia osobom, których dane dotyczą, rzeczywistą możliwość wyboru, jeżeli mogą one wybierać między usługą, która obejmuje wyrażenie zgody na wykorzystywanie ich danych osobowych do celów dodatkowych, z jednej strony, a równoważną usługą oferowaną przez tego samego administratora, która nie obejmuje zgody na wykorzystywanie danych do celów dodatkowych, z drugiej strony. Jeżeli istnieje możliwość wykonania umowy lub świadczenia zleconej usługi przez tego administratora bez konieczności wyrażenia zgody na tego rodzaju inne lub dodatkowe wykorzystanie danych, oznacza to, że usługa nie ma już charakteru warunkowego. Obydwie usługi muszą być jednak faktycznie równoważne.

38. Zdaniem EROD zgody nie można uznać za dobrowolną, jeżeli administrator argumentuje, że istnieje możliwość wyboru między usługą, która obejmuje wyrażenie zgody na wykorzystywanie danych osobowych do celów dodatkowych, z jednej strony, a równoważną usługą oferowaną przez innego administratora, która nie obejmuje zgody na wykorzystywanie danych, z drugiej strony. W takim przypadku swoboda wyboru byłaby zależna od działań innych uczestników rynku oraz od tego, czy konkretna osoba, której dane dotyczą, uznałaby usługi świadczone przez drugiego administratora za faktycznie równoważne. Ponadto nakładałoby to na administratorów obowiązek monitorowania rozwoju sytuacji rynkowej, aby zapewnić ciągłą ważność zgody na podejmowane przez nich czynności przetwarzania danych, ponieważ konkurent może zmienić świadczoną usługę na późniejszym etapie. Co za tym idzie, taka argumentacja oznacza, że zgoda oparta na alternatywnej ofercie proponowanej przez stronę trzecią jest niezgodna z RODO, zatem usługodawca nie może odmówić osobom, których dane dotyczą, dostępu do usługi na podstawie odmowy udzielenia przez nie zgody.

39. Aby spełniony został warunek dobrowolnej zgody, dostęp do usług i funkcji nie może być uzależniony od zgody użytkownika na przechowywanie informacji lub uzyskanie dostępu do informacji już przechowywanych w urządzeniu końcowym użytkownika (tzw. *cookie wall*)[27].

40. Przykład 6a: Dostawca strony internetowej wprowadza skrypt, który powoduje, że zamiast zawartości strony pojawia się prośba o wyrażenie zgody na pliki cookie, a także informacje o działających plikach cookie oraz o celach przetwarzania danych. Nie ma możliwości oglądania zawartości strony bez kliknięcia przycisku „Akceptuję". Ponieważ osobie, której dane dotyczą, nie daje się prawdziwego wyboru, jej zgoda nie zostaje wyrażona dobrowolnie.

41. Wyrażona w ten sposób zgoda jest nieważna, ponieważ dostarczenie usługi zależy od kliknięcia przez osobę, której dane dotyczą, przycisku „Akceptuję". Osoba ta nie ma prawdziwego wyboru.

[25] Zob. także art. 7 ust. 1 RODO, który stanowi, że administrator musi wykazać, iż zgoda osoby, której dane dotyczą, była dobrowolna.

[26] W pewnym stopniu wprowadzenie tego ustępu stanowi kodyfikację istniejących wytycznych GR29. Jak opisano w opinii 15/2011, jeżeli osoba, której dane dotyczą, znajduje się w sytuacji zależności od administratora danych ze względu na charakter relacji lub szczególne okoliczności, może istnieć silne domniemanie, że w takich sytuacjach dobrowolność zgody jest ograniczona (np. w przypadku stosunku pracy lub gromadzenia danych przez organ publiczny). Jeżeli art. 7 ust. 4 ma zastosowanie, administratorowi będzie trudniej udowodnić, że osoba, której dane dotyczą, udzieliła dobrowolnej zgody. Zob. opinia Grupy Roboczej Art. 29 15/2011 w sprawie definicji zgody (WP 187), s.12–17.

[27] Jak wyjaśniono powyżej, określone w RODO przesłanki uzyskania ważnej zgody mają zatem zastosowanie w sytuacjach objętych zakresem stosowania dyrektywy o prywatności i łączności elektronicznej.

3.1.3 Szczegółowość

42. Usługa może obejmować wiele operacji przetwarzania w więcej niż jednym celu. W takich przypadkach osobom, których dane dotyczą, powinna przysługiwać swoboda wyboru celu, który akceptują, zamiast obowiązku wyrażenia zgody na szereg celów przetwarzania. W danym przypadku zgodnie z RODO uzasadnione może być wyrażenie kilku zgód w celu rozpoczęcia oferowania usługi.

43. W motywie 43 wyjaśniono, że zgody nie uważa się za dobrowolną, jeżeli proces/procedura uzyskania zgody uniemożliwia osobom, których dane dotyczą, wyrażenie osobnej zgody odpowiednio na różne operacje przetwarzania danych osobowych (np. wyłącznie na niektóre operacje przetwarzania, z wyłączeniem pozostałych), chociaż w danym przypadku byłoby to w właściwe. Motyw 32 stanowi, że: „[z]goda powinna dotyczyć wszystkich czynności przetwarzania dokonywanych w tym samym celu lub w tych samych celach. Jeżeli przetwarzanie służy różnym celom, potrzebna jest zgoda na wszystkie te cele".

44. Jeżeli administrator połączył kilka celów przetwarzania i nie zwrócił się o osobną zgodę na każdy z tych celów, osoba, której dane dotyczą, jest pozbawiona swobody wyboru. Wspomniana szczegółowość jest ściśle związana z faktem, że zgoda musi być konkretna, jak omówiono w sekcji 3.2 poniżej. W przypadku przetwarzania danych do kilku celów rozwiązaniem umożliwiającym spełnienie przesłanek ważnej zgody jest szczegółowość, tj. rozdzielenie tych celów i uzyskanie zgody na każdy z nich.

45. Przykład 7: W jednym zapytaniu o zgodę sprzedawca detaliczny zwraca się do klientów o wyrażenie zgody na wykorzystywanie ich danych do celów marketingu elektronicznego oraz na udostępnianie tych danych innym przedsiębiorstwom należącym do grupy. Tego rodzaju zgoda nie jest szczegółowa, ponieważ klient nie wyraża osobnej zgody na te dwa odrębne cele, a zatem zgoda jest nieważna. W tym przypadku należy uzyskać konkretną zgodę na przekazanie danych kontaktowych partnerom handlowym. Tego rodzaju konkretna zgoda zostanie uznana za ważną w odniesieniu do każdego z partnerów (zob. również sekcja 3.3.1), o którego tożsamości poinformowano osobę, której dane dotyczą, w chwili wyrażania zgody, o ile zostanie mu ona przekazana w tym samym celu (w niniejszym przykładzie: do celów marketingowych).

3.1.4 Niekorzystne konsekwencje

46. Administrator musi wykazać możliwość odmówienia lub wycofania zgody bez niekorzystnych konsekwencji (motyw 42). Na przykład administrator musi udowodnić, że wycofanie zgody nie pociąga za sobą żadnych kosztów dla osoby, której dane dotyczą, a zatem nie wiąże się z żadną wyraźną szkodą dla osób wycofujących zgodę.

47. Inne przykłady niekorzystnych konsekwencji obejmują wprowadzenie w błąd, zastraszanie, przymus lub znaczące negatywne skutki dla osoby, której dane dotyczą i która nie wyraziła zgody. Administrator powinien być w stanie udowodnić, że osobie, której dane dotyczą, przysługiwała swoboda wyboru lub faktyczna możliwość wyboru co do udzielenia zgody i że miała możliwość wycofania zgody bez niekorzystnych konsekwencji.

48. Jeżeli administrator może wykazać, że usługa obejmuje możliwość wycofania zgody bez żadnych negatywnych konsekwencji, tj. bez obniżenia jakości usługi na szkodę użytkownika, może to świadczyć o dobrowolnym wyrażeniu zgody. RODO nie wyklucza wszystkich zachęt, jednak ciężar udowodnienia dobrowolnego charakteru zgody we wszystkich okolicznościach spoczywałby na administratorze.

49. Przykład 8: Podczas pobierania lifestylowa aplikacja mobilna prosi o wyrażenie zgody na dostęp do miernika przyspieszenia telefonu. Nie jest to konieczne do funkcjonowania aplikacji, ale użyteczne dla administratora, który chciałby uzyskać więcej informacji na temat przemieszczeń i poziomów aktywności użytkowników aplikacji. W przypadku wycofania zgody przez użytkowniczkę okazuje się, że aplikacja działa obecnie jedynie w ograniczonym zakresie. Jest to przykład niekorzystnych konsekwencji w rozumieniu motywu 42, co oznacza, że zgoda nie została uzyskana w sposób ważny (a zatem administrator musi wykasować wszystkie zgromadzone w ten sposób dane osobowe dotyczące przemieszczeń użytkowników).

50. Przykład 9: Osoba, której dane dotyczą, dokonuje subskrypcji biuletynu detalisty odzieżowego oferującego ogólne zniżki. Detalista zwraca się do osoby, której dane dotyczą, o zgodę na gromadzenie większej ilości danych na temat jej preferencji zakupowych, aby dostosować oferty do jej preferencji na podstawie historii zakupów lub kwestionariusza, którego wypełnienie jest dobrowolne. Jeżeli osoba, której dane dotyczą, wycofa następnie zgodę, otrzyma ponownie niespersonalizowane zniżki odzieżowe. Nie można uznać tego faktu za niekorzystne konsekwencje, ponieważ utracono jedynie dopuszczalną zachętę.

51. Przykład 10: Magazyn o modzie oferuje czytelnikom dostęp do nowych produktów do makijażu przed ich oficjalnym wprowadzeniem na rynek.

52. Produkty będą wkrótce dostępne w sprzedaży, jednak czytelnicy magazynu mogą uczestniczyć w ekskluzywnej możliwości wypróbowania tych produktów. Aby skorzystać z tej oferty, muszą oni podać swój adres korespondencyjny i wyrazić zgodę na umieszczenie na liście dystrybucyjnej magazynu. Adres korespondencyjny jest niezbędny do wysyłki, natomiast lista dystrybucyjna jest wykorzystywana w celu wysyłania ofert handlowych produktów, takich jak kosmetyki czy koszulki, przez cały rok.

53. Przedsiębiorstwo wyjaśnia, że dane dostępne na liście dystrybucyjnej będą wykorzystywane wyłącznie do wysyłania towarów i innych reklam w formie papierowej przez sam magazyn i nie zostaną udostępnione żadnej innej organizacji.

54. Jeżeli czytelnik nie chce ujawnić swojego adresu z tego powodu, nie poniesie żadnych niekorzystnych konsekwencji, ponieważ i tak będzie miał dostęp produktów.

3.2 Konkretność

55. W art. 6 ust. 1 lit. a) potwierdzono, że osoba, której dane dotyczą, musi wyrazić zgodę „w jednym lub większej liczbie określonych celów" oraz że osobie tej przysługuje możliwość wyboru w odniesieniu do każdego z nich[28]. Wymóg, zgodnie z którym zgoda musi być „konkretna", ma na celu zapewnienie określonego stopnia kontroli sprawowanej przez użytkownika oraz przejrzystości w odniesieniu do osoby, której dane dotyczą. Wymóg ten nie został zmieniony na mocy RODO i pozostaje ściśle powiązany z wymogiem udzielenia „świadomej" zgody. Jednocześnie należy go interpretować zgodnie z wymogiem dotyczącym „szczegółowości" w celu uzyskania „dobrowolnej" zgody[29]. Podsumowując, aby spełnić wymóg „konkretności" zgody, administrator musi pamiętać o:

i. określeniu celu jako zabezpieczeniu przed zmianą celu;

ii. szczegółowości w zapytaniach o zgodę; oraz

iii. wyraźnym oddzieleniu informacji związanych z uzyskaniem zgody na czynności przetwarzania danych od informacji na inne tematy.

56. **Ad. (i):** Zgodnie z art. 5 ust. 1 lit. b) RODO uzyskanie ważnej zgody jest zawsze poprzedzone określeniem konkretnego, wyraźnego i prawnie uzasadnionego celu zamierzonej czynności przetwarzania[30]. Konieczność uzyskania konkretnej zgody w połączeniu z pojęciem ograniczenia celu zawartym w art. 5 ust. 1 lit. b) stanowi zabezpieczenie przed stopniowym rozszerzaniem lub zacieraniem celów, w których dane są przetwarzane, po wyrażeniu przez osobę, której dane dotyczą, zgody na pierwotne gromadzenie danych. Zjawisko to, znane również jako zmiana celu, stanowi ryzyko dla osób, których dane dotyczą, ponieważ może prowadzić do niespodziewanego wykorzystania danych osobowych przez administratora lub przez osoby trzecie oraz do utraty kontroli przez osobę, której dane dotyczą.

57. Jeżeli administrator opiera się na art. 6 ust. 1 lit. a), osoby, których dane dotyczą, muszą zawsze wyrazić zgodę na konkretny cel przetwarzania[31]. Zgodnie z koncepcją „ograniczenia celu" określoną w art. 5 ust. 1 lit. b) i motywie 32 zgoda może obejmować różne operacje, o ile operacje te służą temu samemu celowi. Nie ulega wątpliwości, że konkretną zgodę można uzyskać wyłącznie wówczas, gdy osoby, których dane dotyczą, zostaną konkretnie poinformowane o zamierzonych celach wykorzystywania danych, które ich dotyczą.

58. Niezależnie od przepisów dotyczących zgodności celów zgoda musi dotyczyć konkretnego celu. Osoby, których dane dotyczą, wyrażą zgodę, zakładając, że sprawują nad nimi kontrolę i że ich dane będą przetwarzane wyłącznie w tych określonych celach. Jeżeli administrator przetwarza dane na podstawie zgody i chciałby przetwarzać dane w nowym celu, musi zwrócić się do osoby, której dane dotyczą, o dodatkową zgodę na ten inny cel, chyba że istnieje inna zgodna z prawem podstawa, która lepiej odzwierciedla sytuację.

59. Przykład 11: Sieć telewizji kablowej gromadzi dane osobowe abonentów na podstawie ich zgody, aby przedstawiać im spersonalizowane propozycje nowych filmów, które mogą ich zainteresować, w oparciu o ich upodobania w zakresie oglądanych programów. Po pewnym czasie sieć telewizyjna decyduje, że chciałaby umożliwić osobom trzecim wysyłanie (lub wyświetlanie) reklamy

[28] Dalsze wskazówki na temat określania „celów" są dostępne w opinii 3/2013 w sprawie ograniczenia celu (WP 203).

[29] Motyw 43 RODO stanowi, że w stosownych przypadkach konieczne będzie uzyskanie osobnej zgody na różne operacje przetwarzania.
Należy zapewnić osobom, których dane dotyczą, możliwość wyrażenia szczegółowej zgody, aby umożliwić im udzielenie osobnej zgody na osobne cele.

[30] Zob. opinia GR29 3/2013 w sprawie ograniczenia celu (WP 203), s. 16: „Z tych powodów cel, który jest niejednoznaczny lub ogólny, taki jak na przykład »poprawa doświadczeń użytkowników«, »cele marketingowe«, »cele bezpieczeństwa informatycznego« lub »przyszłe badania« – bez podania szczegółów – co do zasady nie będzie spełniał kryteriów »konkretności«".

[31] Jest to zgodne z opinią GR29 15/2011 w sprawie definicji zgody (WP 187), np. s. 17.

ukierunkowanej na podstawie upodobań abonentów w zakresie oglądanych programów. Zważywszy na nowy cel, potrzebna jest nowa zgoda.

60. **Ad. (ii):** Aby spełnić wymóg „dobrowolności", mechanizmy zgody muszą być nie tylko szczegółowe, ale muszą również posiadać przymiot „konkretności". Oznacza to, że administrator, który prosi o zgodę na przetwarzanie w wielu różnych celach, powinien zapewnić możliwość wyrażenia zgody osobno na każdy z tych celów, aby umożliwić użytkownikom wyrażenie konkretnej zgody na konkretne cele.

61. **Ad. (iii):** Ponadto w każdym osobnym zapytaniu o zgodę administratorzy powinni podać szczegółowe informacje na temat danych, które są przetwarzane w każdym z celów, aby uświadomić osobom, których dane dotyczą, skutki poszczególnych wyborów, jakich mogą dokonać. Osoby, których dane dotyczą, mogą zatem wyrazić konkretną zgodę. Kwestia ta pokrywa się z wymogiem, aby administratorzy zapewniali jednoznaczne informacje, jak omówiono w pkt 3.3 poniżej.

3.3 Świadoma

62. W RODO wzmocniono wymóg, zgodnie z którym zgoda musi być świadoma. Zgodnie z art. 5 RODO wymóg przejrzystości stanowi jedną z podstawowych zasad, ściśle związaną z zasadami rzetelności i zgodności z prawem. Zapewnianie informacji osobom, których dane dotyczą, przed uzyskaniem ich zgody jest niezbędne do umożliwienia im podejmowania świadomych decyzji, zrozumienia, na co wyrażają zgodę, oraz na przykład wykonania przysługującego im prawa wycofania zgody. Jeżeli administrator nie zapewnia dostępnych informacji, kontrola ze strony użytkownika staje się złudna, a zgoda będzie nieważną podstawą przetwarzania.

63. Konsekwencją niespełnienia wymogów dotyczących świadomej zgody będzie nieważność zgody i możliwość naruszenia przez administratora art. 6 RODO.

3.3.1 Minimalne wymogi dotyczące treści, aby zgoda była „świadoma"

64. Aby zgoda była świadoma, należy poinformować osobę, której dane dotyczą, o określonych elementach kluczowych w celu dokonania wyboru. W związku z tym EROD jest zdania, że do uzyskania ważnej zgody wymagane są przynajmniej następujące informacje:

i. tożsamość administratora;[32]

ii. cel każdej operacji przetwarzania, w odniesieniu do której prosi się o zgodę[33];

iii. jakie dane (jaki rodzaj danych) będą gromadzone i wykorzystywane;[34]

iv. istnienie prawa do wycofania zgody[35];

[32] Zob. także motyw 42 RODO: „[…] Aby wyrażenie zgody było świadome, osoba, której dane dotyczą, powinna znać przynajmniej tożsamość administratora oraz zamierzone cele przetwarzania danych osobowych […]".

[33] Zob. ponownie motyw 42 RODO.

[34] Zob. także opinia GR29 15/2011 w sprawie definicji zgody (WP 187), s. 19–20.

[35] Zob. art. 7 ust. 3 RODO.

v. informacje dotyczące wykorzystywania danych do celów zautomatyzowanego podejmowania decyzji zgodnie z art. 22 ust. 2 lit. c)[36] w stosownych przypadkach; oraz

vi. informacje dotyczące możliwych zagrożeń związanych z przekazywaniem danych w związku z brakiem decyzji stwierdzającej odpowiedni stopień ochrony oraz odpowiednich zabezpieczeń zgodnie z art. 46.[37]

65. Jeżeli chodzi o ppkt (i) i (iii), EROD zauważa, że w przypadku gdy na wnioskowanej zgodzie ma się opierać wielu (współ-)administratorów lub gdy dane mają zostać przekazane innym administratorom lub przetwarzane przez innych administratorów, którzy chcą się opierać na pierwotnej zgodzie, wszystkie te organizacje powinny być wymienione. Podmioty przetwarzające nie muszą być wymienione w ramach wymogów dotyczących zgody, chociaż w celu zapewnienia zgodności z art. 13 i 14 RODO administratorzy będą musieli przedstawić pełen wykaz odbiorców lub kategorii odbiorców, w tym podmiotów przetwarzających. Podsumowując, EROD zauważa, że w zależności od okoliczności i kontekstu sprawy konieczne może być zapewnienie większej ilości informacji, aby umożliwić osobom, których dane dotyczą, rzeczywiste zrozumienie danych operacji przetwarzania.

3.3.2 W jaki sposób należy przekazywać informacje?

66. W RODO nie określono formy przekazywania informacji ani ich kształtu w celu spełnienia wymogu świadomej zgody. Oznacza to, że ważne informacje mogą być przekazane na różne sposoby, np. w formie pisemnych lub ustnych oświadczeń bądź wiadomości dźwiękowych lub wiadomości wideo. W RODO ustanowiono jednak szereg wymogów dotyczących świadomej zgody, głównie w art. 7 ust. 2 i motywie 32. Prowadzi to do wyższego standardu jasności i dostępności informacji.

67. Prosząc o zgodę, administratorzy powinni się upewnić, że używają jasnego i prostego języka we wszystkich przypadkach. Oznacza to, że wiadomość powinna być zrozumiała dla przeciętnej osoby, a nie tylko dla prawników. Administratorzy nie mogą stosować długich i trudnych w zrozumieniu informacji o polityce prywatności ani zamieszczać w nich oświadczeń pełnych żargonu prawniczego. Zgoda musi być jednoznaczna i udzielona w sposób pozwalający wyraźnie odróżnić ją od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie. Wymóg ten oznacza co do zasady, że informacje istotne dla podjęcia świadomych decyzji o wyrażeniu lub niewyrażeniu zgody nie mogą być ukryte w ogólnych warunkach[38].

68. Administrator danych musi dopilnować, aby osoby, których dane dotyczą, wyrażały zgodę na podstawie informacji, które pozwalają im na łatwą identyfikację administratora danych oraz zrozumienie, na co wyrażają zgodę. Administrator musi jasno opisać cel przetwarzania danych, którego dotyczy zapytanie o zgodę[39].

[36] Zob. także wytyczne GR29 w sprawie zautomatyzowanego podejmowania decyzji i profilowania do celów rozporządzenia 2016/679 (WP 251), pkt IV.B, s. 20 i nast.

[37] Zgodnie z art. 49 ust. 1 lit. a) w przypadku zwrócenia się o wyraźną zgodę wymagane są szczegółowe informacje na temat braku zabezpieczeń opisanych w art. 46. Zob. także opinia GR29 15/2011 w sprawie definicji zgody (WP 187), s. 19.

[38] Oświadczenie o wyrażeniu zgody musi być określone jako takie. Sformułowania, takie jak „Wiem, że…", nie spełniają wymogów jasnego języka.

[39] Zob. art. 4 pkt 11 oraz art. 7 ust. 2 RODO.

69. Inne szczegółowe wskazówki dotyczące dostępności przedstawiono w wytycznych GR29 w sprawie przejrzystości. Jeżeli zgoda ma zostać wyrażona drogą elektroniczną, zapytanie musi być jasne i zwięzłe. Wielowarstwowe i szczegółowe informacje mogą być właściwym sposobem wywiązania się z podwójnego obowiązku obejmującego z jednej strony precyzyjność i kompletność, a z drugiej strony zrozumiałość.

70. Administrator musi ocenić, jaki rodzaj odbiorców przekazuje swoje dane osobowe jego organizacji. Przykładowo, w przypadku gdy do grupy docelowej należą małoletnie osoby, których dane dotyczą, administrator danych powinien dopilnować, aby informacje były zrozumiałe dla małoletnich[40]. Po określeniu swoich odbiorców administratorzy muszą ustalić, jakie informacje powinni dostarczyć, a następnie w jaki sposób przedstawią informacje osobom, których dane dotyczą.

71. Art. 7 ust. 2 odnosi się do uprzednio sformułowanych pisemnych oświadczeń o wyrażeniu zgody, które dotyczą także innych kwestii. Gdy o zgodę prosi się w ramach umowy (na papierze), zapytanie o zgodę powinno się wyraźnie odróżniać od pozostałych kwestii. Jeżeli umowa na papierze obejmuje wiele aspektów niezwiązanych z kwestią zgody na wykorzystanie danych osobowych, kwestia zgody powinna zostać przedstawiona w wyraźnie odróżniający się sposób lub w odrębnym dokumencie. Podobnie, jeżeli o zgodę prosi się drogą elektroniczną, zapytanie o zgodę musi być odrębne i możliwe do odróżnienia – nie może to być po prostu jeden akapit w warunkach, zgodnie z motywem 32[41]. Aby zapewnić dostosowanie do małych ekranów lub sytuacji, w których miejsce na informacje jest ograniczone, w stosownych przypadkach można rozważyć warstwowy sposób przedstawienia informacji, aby uniknąć nadmiernego wpływu na funkcjonalność lub koncepcję produktu.

72. Administrator, który polega na zgodzie osoby, której dane dotyczą, musi również wywiązać się z odrębnych obowiązków informacyjnych ustanowionych w art. 13 i 14, aby zapewnić zgodność z RODO. W praktyce wywiązanie się z obowiązków informacyjnych i spełnienie wymogu uzyskania świadomej zgody może w wielu przypadkach prowadzić do przyjęcia zintegrowanego podejścia. Niniejszą sekcję sporządzono jednak przy założeniu, że ważna, „świadoma" zgoda może istnieć nawet wówczas, gdy nie wszystkie elementy określone w art. 13 lub 14 zostaną wspomniane w procesie uzyskiwania zgody (punkty te należy oczywiście wskazać w innych miejscach, takich jak informacje o polityce prywatności przedsiębiorstwa). GR29 wydała odrębne wytyczne dotyczące wymogu przejrzystości.

73. Przykład 12: Przedsiębiorstwo X jest administratorem, który otrzymał skargi, że nie jest jasne dla osób, których dane dotyczą, na jakie rodzaje wykorzystywania danych są proszeni o zgodę. Przedsiębiorstwo dostrzega potrzebę sprawdzenia, czy informacje zawarte w zapytaniu o zgodę są zrozumiałe dla osób, których dane dotyczą. Przedsiębiorstwo X organizuje dobrowolne panele testowe wśród konkretnych kategorii swoich klientów i przedstawia uczestnikom testów nowe zaktualizowane informacje dotyczące zgody przed ogłoszeniem ich na zewnątrz. Wybór kategorii klientów dokonywany jest zgodnie z zasadą niezależności oraz w oparciu o standardy zapewniające reprezentatywny, bezstronny wynik. Klienci otrzymują kwestionariusz i wskazują, co zrozumieli z przedstawionych informacji oraz w jaki sposób oceniliby je pod względem zrozumiałości i istotności informacji. Administrator kontynuuje testy do czasu, aż uczestnicy stwierdzą, że informacje są zrozumiałe. Przedsiębiorstwo X sporządza sprawozdanie z testu i umożliwia dostęp do niego w przyszłości. Przykład ten pokazuje możliwy sposób wykazania przez przedsiębiorstwo X, że osoby, których dane dotyczą, otrzymywały jasne informacje przed wyrażeniem zgody na przetwarzanie danych osobowych przez przedsiębiorstwo X.

74. Przykład 13: Przedsiębiorstwo przetwarza dane na podstawie zgody. Stosuje ono warstwowe informacje o polityce prywatności obejmujące zapytanie o zgodę. Przedsiębiorstwo ujawnia wszystkie podstawowe informacje na temat administratora oraz planowanych czynności przetwarzania danych[42]. Przedsiębiorstwo nie wskazuje jednak w pierwszej warstwie informacji o polityce prywatności, w jaki sposób można się skontaktować z jego inspektorem ochrony danych. Aby mieć ważną, zgodną z prawem podstawę w rozumieniu art. 6, administrator ten uzyskał ważną „świadomą" zgodę, nawet jeśli dane kontaktowe inspektora ochrony danych nie zostały przekazane osobie, której dane dotyczą, (w pierwszej warstwie informacji) zgodnie z art. 13 ust. 1 lit. b) lub art. 14 ust. 1 lit. b) RODO.

3.4 Jednoznaczne okazanie woli

75. Z RODO wyraźnie wynika, że zgoda wymaga oświadczenia osoby, której dane dotyczą, lub wyraźnego działania potwierdzającego, co oznacza, że musi być zawsze udzielona przez aktywne działanie lub oświadczenie. Musi być oczywiste, że osoba, której dane dotyczą, zgodziła się na określone przetwarzanie.

76. W art. 2 lit. h) dyrektywy 95/46/WE opisano zgodę jako „wskazanie przez osobę, której dane dotyczą na to, że wyraża przyzwolenie na przetwarzanie odnoszących się do niej danych osobowych". Opierając się na tej definicji, w art. 4 pkt 11 RODO wyjaśniono, że ważna zgoda wymaga „jednoznacznego" okazania woli w formie „oświadczenia lub wyraźnego działania potwierdzającego" zgodnie z poprzednimi wytycznymi wydanymi przez GR29.

77. „Wyraźne działanie potwierdzające" oznacza, że osoba, której dane dotyczą, musiała podjąć celowe działanie, aby wyrazić zgodę na określone przetwarzanie[43]. Motyw 32 zawiera dodatkowe wskazówki

[40] Zob. także motyw 58 dotyczący informacji zrozumiałych dla dzieci.

[41] Zob. także motyw 42 i dyrektywa 93/13/WE, w szczególności jej art. 5 (prosty i zrozumiały język, interpretacja wszelkich wątpliwości na korzyść konsumenta) oraz art. 6 (nieważność nieuczciwych postanowień umownych, umowa będzie nadal obowiązywała bez tych postanowień wyłącznie wówczas, gdy będzie to zasadne, w przeciwnym razie cała umowa będzie nieważna).

[42] Należy zauważyć, że gdy tożsamość administratora lub cel przetwarzania danych nie wynikają z pierwszej warstwy informacyjnej warstwowych informacji o polityce prywatności (i znajdują się w kolejnych warstwach), administratorowi danych trudno będzie wykazać, że osoba, której dane dotyczą, udzieliła świadomej zgody, chyba że administrator danych jest w stanie wykazać, iż osoba ta uzyskała dostęp do tych informacji przed udzieleniem zgody.

[43] Zob. dokument roboczy służb Komisji, ocena skutków, załącznik 2, s. 20, a także s. 105–106: „Jak również wskazano w przyjętej przez GR29 opinii w sprawie zgody, kluczowe wydaje się wyjaśnienie, że ważna zgoda wymaga zastosowania mechanizmów, które nie pozostawiają wątpliwości co do woli wyrażenia zgody przez osobę, której dane dotyczą, przy jednoczesnym sprecyzowaniu, że – w kontekście otoczenia elektronicznego – wykorzystanie domyślnych ustawień, które osoba, której dane dotyczą, musi zmodyfikować, aby odmówić przetwarzania (»zgoda oparta na milczeniu«), nie stanowi samo w sobie jednoznacznej zgody. Zapewniłoby to poszczególnym osobom większą kontrolę nad ich własnymi danymi, niezależnie od tego, czy przetwarzanie opiera się na ich zgodzie. Jeżeli chodzi o administratorów danych, nie miałoby to na nich większego wpływu, ponieważ chodzi wyłącznie o wyjaśnienie i lepsze wysłowienie skutków obowiązującej dyrektywy w odniesieniu do przesłanek ważnej i znaczącej zgody uzyskanej od osoby, której dane dotyczą. W szczególności w zakresie, w jakim pojęcie »wyraźnej« zgody precyzowałoby – przez zastąpienie określenia »jednoznaczna« – warunki i jakość zgody oraz nie miałoby na celu rozszerzenia zakresu przypadków i sytuacji, w których należy wykorzystać (wyraźną) zgodę jako podstawę przetwarzania, nie oczekuje się, aby wpływ tego środka na administratorów danych był znaczny".

w tym zakresie. Zgodę można uzyskać w formie pisemnego lub (zarejestrowanego) ustnego oświadczenia, w tym drogą elektroniczną.

78. Być może najbardziej dosłownym sposobem spełnienia kryterium „pisemnego oświadczenia" jest zapewnienie, by osoba, której dane dotyczą, wysłała pismo lub wiadomość e-mail do administratora, wyjaśniając, na co dokładnie się zgadza. Często jest to jednak nierealne. Oświadczenia pisemne mogą przybierać różne formy i rozmiary, które mogłyby być zgodne z RODO.

79. Bez uszczerbku dla istniejącego (krajowego) prawa umów zgodę można uzyskać w formie zarejestrowanego oświadczenia ustnego, chociaż przed wyrażeniem zgody należy właściwie uwzględnić informacje dostępne dla osoby, której dane dotyczą. Zastosowanie wcześniej zaznaczonych pól ze zgodą jest nieważne na mocy RODO. Milczenie lub bezczynność po stronie osoby, której dane dotyczą, jak również po prostu kontynuowanie korzystania z usługi nie mogą zostać uznane za aktywne wskazanie wyboru.

80. Przykład 14: Przy instalowaniu oprogramowania aplikacja prosi osobę, której dane dotyczą, o zgodę na stosowanie niezanonimizowanych raportów o awarii w celu usprawnienia oprogramowania. Zapytaniu o zgodę towarzyszą warstwowe informacje o polityce prywatności zawierające niezbędne wyjaśnienia. Zaznaczając opcjonalne pole o treści „Wyrażam zgodę", użytkownik jest w stanie dokonać ważnego „wyraźnego działania potwierdzającego" w celu wyrażenia zgody na przetwarzanie.

81. Administrator musi również mieć świadomość, że zgody nie można uzyskać w drodze tej samej czynności co zawarcie umowy czy zaakceptowanie ogólnych warunków usługi. Zbiorczego zaakceptowania ogólnych warunków nie można uznać za wyraźne działanie potwierdzające wyrażenie zgody na wykorzystanie danych osobowych. RODO nie dopuszcza możliwości stosowania przez administratorów wcześniej zaznaczonych pól ani mechanizmów opt-out (możliwość rezygnacji), które wymagają ingerencji ze strony osoby, której dane dotyczą, w celu uniemożliwienia zawarcia umowy (na przykład pola *opt-out*)[44].

82. Jeżeli zgoda ma zostać wyrażona w odpowiedzi na elektroniczne zapytanie o zgodę, zapytanie takie nie powinno zakłócać *niepotrzebnie* korzystania z usługi, której dotyczy[45]. Dokonana w czynny sposób czynność potwierdzająca, za pośrednictwem której osoba, której dane dotyczą, wyraża zgodę, może być konieczna, jeżeli mniej inwazyjny lub zakłócający sposób powodowałby niejednoznaczność. Konieczne może być zatem, aby zapytanie o zgodę zakłóciło w pewnym stopniu korzystanie z usługi w celu zapewnienia skuteczności zapytania.

83. Zgodnie z wymogami RODO administratorzy mają jednak swobodę w zakresie opracowania procedury wyrażania zgody odpowiedniej dla ich organizacji. W tym zakresie fizyczne działania można zakwalifikować jako wyraźne działania potwierdzające zgodnie z RODO.

84. Administratorzy powinni opracować mechanizmy zgody w sposób, który jest jednoznaczny dla osób, których dane dotyczą. Administratorzy muszą unikać niejednoznaczności i zapewnić, by czynność, za pośrednictwem której udzielana jest zgoda, można było odróżnić od innych czynności. W związku z tym samo kontynuowanie zwykłego korzystania ze strony internetowej nie jest zachowaniem, na podstawie którego można wywnioskować okazanie woli przez osobę, której dane dotyczą, polegające na wyrażeniu zgody na proponowaną operację przetwarzania.

[44] Zob. art. 7 ust. 2. Zob. także dokument roboczy 02/2013 w sprawie uzyskiwania zgody na pliki cookie (WP 208), s. 3–6.

[45] Zob. motyw 32 RODO.

85. Przykład 15: Przesunięcie paska na ekranie, machnięcie przed inteligentną kamerą, obrócenie smartfona zgodnie z ruchem wskazówek zegara lub zakreślenie ósemki mogą być wariantami wyrażenia zgody, o ile zapewnione są jasne informacje i nie ulega wątpliwości, że dany ruch oznacza zgodę w odpowiedzi na konkretne zapytanie (np. „Przesunięcie paska w lewo oznacza zgodę na wykorzystanie informacji X w celu Y. Należy powtórzyć ruch w celu potwierdzenia."). Administrator musi być w stanie wykazać, że zgodę uzyskano w ten sposób, a osoby, których dane dotyczą, muszą mieć możliwość wycofania zgody tak łatwo, jak jej udzieliły.

86. Przykład 16: W myśl motywu 32 przewijanie w dół, przeglądanie strony internetowej lub podobne działania użytkownika w żadnych okolicznościach nie spełniają wymogu wyraźnego i potwierdzającego działania: działania takie może być trudno odróżnić od innych działań lub reakcji użytkownika, a zatem niemożliwe również będzie stwierdzenie, że uzyskano jednoznaczną zgodę. Ponadto, w takim przypadku trudne będzie zapewnienie użytkownikowi możliwości wycofania zgody w sposób równie łatwy, co jej udzielenie.

87. W kontekście cyfrowym wiele usług potrzebuje do funkcjonowania danych osobowych, w związku z czym osoby, których dane dotyczą, codziennie otrzymują wiele zapytań o zgodę, na które odpowiada się kliknięciem i przesunięciem. Może to doprowadzić do zmęczenia klikaniem: gdy ma się z nim do czynienia zbyt często, zmniejsza się ich faktyczny skutek ostrzeżenia.

88. Prowadzi to do sytuacji, w której zapytania o zgodę nie są już czytane. Stanowi to szczególne ryzyko dla osób, których dane dotyczą, ponieważ zazwyczaj zapytania o zgodę dotyczą działań, które są co do zasady niezgodne z prawem w przypadku braku zgody. W RODO nałożono na administratorów obowiązek opracowania sposobów radzenia sobie z tą kwestią.

89. Często wymienianym przykładem, jak to zrobić w kontekście internetowym, jest uzyskanie zgody użytkowników internetu za pośrednictwem ich ustawień przeglądarki. Takie ustawienia powinny być opracowane zgodnie z przesłankami ważnej zgody określonymi w RODO, takimi jak na przykład fakt, że zgoda powinna być szczegółowa dla każdego z zamierzonych celów oraz że informacje, które mają być przekazane, powinny obejmować informacje o administratorach.

90. W każdym przypadku zgodę należy bezwzględnie uzyskać przed rozpoczęciem przez administratora przetwarzania danych osobowych, na które potrzebna jest zgoda. GR29 konsekwentnie utrzymywała w swoich opiniach, że zgoda powinna być wyrażona przed rozpoczęciem przetwarzania[46]. Chociaż w art. 4 pkt 11 RODO nie przewidziano wyraźnie, że zgoda musi być wyrażona przed rozpoczęciem przetwarzania, jest to jasno dane do zrozumienia. Nagłówek art. 6 ust. 1 oraz sformułowanie „wyraziła" w art. 6 ust. 1 lit. a) wspierają tę interpretację. Z art. 6 oraz motywu 40 wynika logicznie, że ważna, zgodna z prawem podstawa musi istnieć przed rozpoczęciem przetwarzania danych. W związku z tym zgoda powinna być wyrażona przed rozpoczęciem przetwarzania. Co do zasady wystarczające może być jednokrotne zapytanie o zgodę osoby, której dane dotyczą. Administratorzy muszą jednak uzyskać nową i konkretną zgodę, jeżeli cele przetwarzania danych zmienią się po uzyskaniu zgody lub jeżeli planowany jest dodatkowy cel przetwarzania.

[46] GR29 konsekwentnie stała na tym stanowisku od wydania opinii 15/2011 w sprawie definicji zgody (WP 187), s. 30–31.

4 UZYSKANIE WYRAŹNEJ ZGODY

91. Wyraźna zgoda jest wymagana w określonych sytuacjach, gdy pojawia się poważne ryzyko związane z ochroną danych, a zatem w sytuacjach, w których za właściwy uznaje się wysoki poziom indywidualnej kontroli nad danymi osobowymi. Zgodnie z RODO wyraźna zgoda odgrywa istotną rolę w przetwarzaniu szczególnych kategorii danych zgodnie z art. 9, przekazywaniu danych do państw trzecich i organizacji międzynarodowych w przypadku braku odpowiednich zabezpieczeń w art. 49[47] oraz w art. 22 dotyczącym zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach, w tym profilowania[48].

92. Zgodnie z RODO „oświadczenie lub wyraźne działanie potwierdzające" stanowią warunek wstępny „zwykłej" zgody. Ponieważ wymóg dotyczący „zwykłej" zgody określony w RODO został już podniesiony do wyższego standardu w porównaniu z wymogiem dotyczącym zgody określonym w dyrektywie 95/46/WE, należy wyjaśnić, jakie dodatkowe starania powinien podjąć administrator, aby uzyskać „wyraźną" zgodę od osoby, której dane dotyczą, zgodnie z RODO.

93. Termin „wyraźna" odnosi się do sposobu wyrażenia zgody przez osobę, której dane dotyczą. Oznacza to, że osoba, której dane dotyczą, musi złożyć w sposób wyraźny oświadczenie o wyrażeniu zgody. Oczywistym sposobem zapewnienia, aby zgoda była wyraźna, byłoby jej wyraźne potwierdzenie w pisemnym oświadczeniu. W stosownych przypadkach administrator mógłby zapewnić podpisanie pisemnego oświadczenia przez osobę, której dane dotyczą, aby rozwiać wszelkie możliwe wątpliwości i zapobiec możliwemu brakowi dowodów w przyszłości[49].

94. Takie podpisane oświadczenie nie jest jednak jedynym sposobem uzyskania wyraźnej zgody i nie można stwierdzić, iż w RODO przewidziano obowiązek uzyskania pisemnych i podpisanych oświadczeń we wszystkich okolicznościach, w których wymagane jest uzyskanie ważnej wyraźnej zgody. Na przykład w kontekście cyfrowym lub online osoba, której dane dotyczą, może być w stanie złożyć wymagane oświadczenie przez wypełnienie formularza elektronicznego, wysłanie wiadomości e-mail, przesłanie zeskanowanego dokumentu opatrzonego podpisem osoby, której dane dotyczą, lub złożenie podpisu elektronicznego. W teorii wykorzystanie oświadczeń ustnych również może zostać uznane za wystarczająco wyraźny sposób uzyskania ważnej wyraźnej zgody, jednak administratorowi

[47] Zgodnie z art. 49 ust. 1 lit. a) RODO wyraźna zgoda może spowodować uchylenie zakazu przekazywania danych do krajów, których prawo w dziedzinie ochrony danych nie zapewnia odpowiedniego stopnia ochrony. Zob. także dokument roboczy w sprawie wspólnej wykładni art. 26 ust. 1 dyrektywy 95/46/WE z dnia 24 października 1995 r. (WP 114), s. 11, w którym GR29 wskazała, że zgoda na przekazywanie danych, które odbywa się okresowo lub stale, nie jest właściwa.

[48] W art. 22 RODO wprowadzono przepisy chroniące osoby, których dane dotyczą, przed podejmowaniem decyzji opartym wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu. Podejmowanie decyzji na tej podstawie jest dozwolone pod określonymi prawnymi warunkami prawnymi. Zgoda odgrywa kluczową rolę w tym mechanizmie ochrony, ponieważ w art. 22 ust. 2 lit. c) RODO wyjaśniono, że administrator może skorzystać z zautomatyzowanego podejmowania decyzji, w tym profilowania, które może istotnie wpływać na daną osobę, w przypadku udzielenia wyraźnej zgody przez osobę, której dane dotyczą. GR29 przygotowała odrębne wytyczne na ten temat: wytyczne GR29 w sprawie zautomatyzowanego podejmowania decyzji i profilowania do celów rozporządzenia 2016/679, 3 października 2017 r. (WP 251).

[49] Zob. także opinia GR29 15/2011 w sprawie definicji zgody (WP 187), s. 25.

może być trudno udowodnić, że spełniono wszystkie przesłanki ważnej wyraźnej zgody w chwili, gdy przyjmowano oświadczenie.

95. Organizacja może również uzyskać wyraźną zgodę podczas rozmowy telefonicznej, pod warunkiem że informacje dotyczące wyboru są uczciwe, zrozumiałe i jasne i że organizacja zwraca się do osoby, której dane dotyczą, o konkretne potwierdzenie (np. naciśnięcie przycisku lub ustne potwierdzenie).

96. Przykład 17: Administrator danych może również uzyskać wyraźną zgodę od odwiedzającego stronę internetową przez wprowadzenie ekranu umożliwiającego wyrażenie wyraźnej zgody zawierającego pola wyboru „Tak" i „Nie", na przykład „Niniejszym wyrażam zgodę na przetwarzanie moich danych", a nie na przykład „Rozumiem, że moje dane będą przetwarzane". Nie ulega wątpliwości, że należy spełnić przesłanki dotyczące świadomej zgody, jak również pozostałe przesłanki uzyskania ważnej zgody.

97. Przykład 18: Klinika chirurgii plastycznej prosi o wyraźną zgodę do pacjenta na przekazanie jego dokumentacji medycznej ekspertowi, do którego klinika zwraca się o drugą opinię na temat stanu pacjenta. Dokumentacja medyczna jest w formie pliku cyfrowego. Z uwagi na szczególny charakter tych informacji klinika prosi o podpis elektroniczny osobę, której dane dotyczą, w celu uzyskania ważnej wyraźnej zgody oraz aby móc wykazać, że uzyskano wyraźną zgodę[50].

98. Innym sposobem upewnienia się, że wyraźna zgoda jest ważna, jest dwuetapowa weryfikacja zgody. Na przykład osoba, której dane dotyczą, otrzymuje wiadomość e-mail z zawiadomieniem o tym, że administrator danych zamierza przetwarzać rejestr zawierający dane medyczne. Administrator wyjaśnia w wiadomości e-mail, że prosi o zgodę na wykorzystanie określonego zestawu informacji w konkretnym celu. Jeżeli osoba, której dane dotyczą, zgadza się na wykorzystanie tych danych, administrator prosi ją o odpowiedź w formie wiadomości e-mail zawierającej oświadczenie „Wyrażam zgodę". Po wysłaniu odpowiedzi osoba, której dane dotyczą, otrzymuje link weryfikacyjny, który należy kliknąć, lub wiadomość SMS z kodem weryfikacyjnym w celu potwierdzenia zgody.

99. W art. 9 ust. 2 nie przewidziano, by charakter danych „niezbędnych do wykonania umowy" był wyjątkiem od ogólnego zakazu przetwarzania szczególnych kategorii danych. W związku z tym administratorzy i państwa członkowskie, które znajdują się w takiej sytuacji, powinni zbadać konkretne wyjątki przewidziane w art. 9 ust. 2 lit. b)–j). Jeżeli żaden z wyjątków przewidzianych w przepisach lit. b)–j) nie będzie miał zastosowania, jedynym możliwym wyjątkiem, który można zastosować zgodnie z prawem do przetwarzania takich danych, jest uzyskanie wyraźniej zgody zgodnie z przewidzianymi w RODO warunkami uzyskania ważnej zgody.

100. Przykład 19: Przedsiębiorstwo lotnicze Holiday Airways oferuje usługę podróżowania z asystą dla pasażerów, którzy np. ze względu na niepełnosprawność nie mogą podróżować bez asysty. Klientka rezerwuje lot z Amsterdamu do Budapesztu i zwraca się o asystę w podróży, aby móc wejść na pokład samolotu. Holiday Airways prosi klientkę o podanie informacji na temat jej stanu zdrowia, aby móc zorganizować dla niej właściwe usługi (istnieje bowiem wiele możliwości, np. podstawienie wózka inwalidzkiego przy bramce do odlotu lub zapewnienie asystenta, który odbędzie z nią podróż od punktu A do punktu B). Holiday Airways prosi o wyraźną zgodę na przetwarzanie danych dotyczących zdrowia tej klientki do celów zorganizowania żądanej usługi asysty w podróży. Dane przetwarzane na podstawie zgody powinny być niezbędne do realizacji żądanej usługi. Ponadto z lotów do Budapesztu

[50] Przykład ten pozostaje bez uszczerbku dla rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym.

można korzystać bez asysty w podróży. Należy zwrócić uwagę, że ponieważ dane są niezbędne do zapewnienia żądanej usługi, przepisy art. 7 ust. 4 nie mają zastosowania.

101. Przykład 20: Dobrze prosperujące przedsiębiorstwo specjalizuje się w produkcji gogli narciarskich i snowboardowych na zamówienia oraz innych rodzajów spersonalizowanych okularów do uprawiania sportu na świeżym powietrzu. Założeniem jest możliwość korzystania z tych produktów bez konieczności noszenia własnych okularów. Przedsiębiorstwo zbiera zamówienia w swoim punkcie centralnym i dostarcza produkty z jednego miejsca do wszystkich krajów w UE.

102. Aby móc dostarczać spersonalizowane produkty klientom z krótkowzrocznością, ten administrator danych prosi o zgodę na wykorzystywanie informacji na temat stanu wzroku klientów. Klienci przekazują przez internet niezbędne dane dotyczące zdrowia, np. swoje dane z recepty, w momencie składania zamówienia. Bez tych danych dostarczenie zamówionych spersonalizowanych okularów nie byłoby możliwe. Przedsiębiorstwo oferuje również kolekcje gotowych gogli korekcyjnych. Klienci, którzy nie chcą udostępniać swoich danych dotyczących zdrowia, mogą skorzystać z wersji gotowych. A zatem wymagana jest wyraźna zgoda zgodnie z art. 9 i zgodę można uznać za dobrowolną.

5 DODATKOWE WARUNKI UZYSKANIA WAŻNEJ ZGODY

103. W RODO wprowadzono wymogi zapewnienia przez administratorów dodatkowych rozwiązań, aby mogli oni otrzymać i zachować ważną zgodę oraz wykazać jej posiadanie. W art. 7 RODO określono te dodatkowe warunki uzyskania ważnej zgody, w tym przepisy szczegółowe dotyczące przechowywania rejestrów zgód i prawa do łatwego wycofania zgody. Art. 7 stosuje się również do zgód, o których mowa w innych artykułach RODO, np. w art. 8 i 9. Poniżej przedstawiono wskazówki dotyczące dodatkowego wymogu, jakim jest wykazanie ważnej zgody, oraz wycofania zgody.

5.1 Wykazanie zgody

104. W art. 7 ust. 1 RODO jasno wskazano wyraźny obowiązek wykazania przez administratora, że osoba, której dane dotyczą, wyraziła zgodę. Zgodnie z art. 7 ust. 1 ciężar dowodu spoczywa na administratorze.

105. Motyw 42 stanowi, że: „jeśli przetwarzanie odbywa się na podstawie zgody osoby, której dane dotyczą, administrator powinien być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na operację przetwarzania".

106. Administratorzy mogą swobodnie opracowywać metody zapewnienia zgodności z tym przepisem w sposób, który jest spójny z ich bieżącą działalnością. Równocześnie obowiązek wykazania, że administrator uzyskał ważną zgodę, nie powinien sam w sobie prowadzić do nadmiernego przetwarzania dodatkowych danych. Oznacza to, że administratorzy powinni mieć wystarczająco dużo danych, aby móc wykazać związek z przetwarzaniem (aby wykazać, że uzyskano zgodę), ale nie powinni zbierać więcej informacji niż to konieczne.

107. Do administratora należy udowodnienie, że osoba, której dane dotyczą, wyraziła ważną zgodę. W RODO nie określono dokładnie, w jaki sposób należy to zrobić. Administrator musi być jednak w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę w danym przypadku. Dopóki dane są przetwarzane, dopóty istnieje obowiązek wykazania prawidłowo wyrażonej zgody. Po zakończeniu czynności przetwarzania dowód na wyrażenie zgody nie powinien być przechowywany dłużej niż jest to bezwzględnie konieczne do wywiązania się z prawnego obowiązku lub do ustalenia, dochodzenia lub obrony roszczeń zgodnie z art. 17 ust. 3 lit. b) i e).

108. Na przykład administrator może prowadzić rejestr uzyskanych oświadczeń o wyrażeniu zgody, tak aby mógł wykazać, w jaki sposób i kiedy uzyskano zgodę oraz jakie informacje przekazano osobie, której dane dotyczą, w momencie uzyskania zgody. Administrator musi być również w stanie wykazać, że osoba, której dane dotyczą, została poinformowana, a procedura zastosowana przez administratora spełniała wszystkie właściwe kryteria uzyskania ważnej zgody. Argumentem za takim wymogiem w przepisach RODO jest fakt, że to administrator jest odpowiedzialny za uzyskanie ważnej zgody od osób, które dane dotyczą, i wdrożone mechanizmy zgody. Przykładowo w kontekście internetowym administrator mógłby przechowywać informacje na temat sesji, w ramach której udzielono zgodę, wraz z dokumentacją obiegu zgody w czasie tej sesji, jak również kopię informacji przedstawionych wówczas osobie, której dane dotyczą. Niewystarczające byłoby natomiast jedynie odniesienie się do prawidłowej konfiguracji strony internetowej.

109. Przykład 21: Szpital organizuje program badań naukowych pod nazwą „projekt X", do którego realizacji niezbędna jest dokumentacja dentystyczna prawdziwych pacjentów. Uczestników rekrutuje się telefonicznie spośród pacjentów, którzy dobrowolnie zgodzili się na wpisanie ich na listę kandydatów, do których można się zwrócić w tym celu. Administrator prosi osoby, których dane dotyczą, o wyraźną zgodę na wykorzystanie ich dokumentacji dentystycznej. Zgoda zostaje uzyskana w trakcie rozmowy telefonicznej przez nagranie ustnego oświadczenia osoby, której dane dotyczą, w którym osoba ta potwierdza, że zgadza się na wykorzystanie swoich danych do celów projektu X.

110. W RODO nie określono ram czasowych, w których taka zgoda jest ważna. Okres ważności zgody zależy od kontekstu, zakresu pierwotnej zgody i oczekiwań osoby, której dane dotyczą. Jeżeli operacje przetwarzania zmienią się lub ewoluują w sposób znaczący, wówczas pierwotna zgoda nie będzie już ważna. W takim wypadku należy uzyskać nową zgodę.

111. Jako najlepszą praktykę EROD zaleca, by zgoda była aktualizowana we właściwych odstępach czasu. Ponowne przekazanie wszystkich informacji pomaga zapewnić, by osoba, której dane dotyczą, w dalszym ciągu była dobrze poinformowana, w jaki sposób wykorzystywane są jej dane i jak może korzystać ze swoich praw[51].

5.2 Wycofanie zgody

112. Wycofanie zgody zajmuje ważne miejsce w RODO. Przepisy i motywy RODO dotyczące wycofania zgody można uznać za kodyfikację dotychczasowej interpretacji tej kwestii przedstawionej w opiniach GR29[52].

113. Zgodnie z art. 7 ust. 3 RODO administrator musi zapewnić, by osoba, której dane dotyczą, mogła wycofać zgodę z taką samą łatwością, z jaką jej udzieliła, i w dowolnym momencie. W RODO nie stwierdzono, że udzielanie i cofnięcie zgody musi zawsze odbywać się w ten sam sposób.

114. Jeżeli jednak w praktyce zgody udziela się drogą elektroniczną przez jedno kliknięcie myszą, przesunięcie lub kliknięcie klawisza, osoby, których dane dotyczą, muszą mieć możliwość wycofania tej

[51] Zob. wytyczne Grupy Roboczej Art. 29 w sprawie przejrzystości na mocy rozporządzenia 2016/679, WP260 rev.01, zatwierdzone przez EROD.

[52] GR29 omówiła tę kwestię w swojej opinii na temat zgody (zob. opinia 15/2011 w sprawie definicji zgody (WP 187), s. 9, 13, 20, 27 i 32–33) oraz m.in. w opinii w sprawie wykorzystywania danych dotyczących lokalizacji (zob. opinia 5/2005 w sprawie wykorzystywania danych dotyczących lokalizacji w celu świadczenia usług tworzących wartość dodaną (WP 115), s. 7).

zgody w równie łatwy sposób. W przypadku gdy zgoda jest uzyskiwana za pomocą interfejsu użytkownika odrębnego dla danej usługi (np. poprzez stronę internetową, aplikację, konto logowania, interfejs urządzenia IoT lub pocztę elektroniczną), nie ulega wątpliwości, że osoba, której dane dotyczą, musi być w stanie wycofać zgodę poprzez ten sam interfejs elektroniczny, ponieważ przełączenie się na inny interfejs wyłącznie w celu wycofania zgody wymagałoby zbędnego wysiłku. Ponadto osoba, której dane dotyczą, powinna być w stanie wycofać zgodę bez ponoszenia niekorzystnych konsekwencji. Oznacza to m.in. że administrator musi zapewnić, by wycofanie zgody było bezpłatne lub nie pociągało za sobą obniżenia poziomu usług[53].

115. Przykład 22: Festiwal muzyczny sprzedaje bilety za pośrednictwem platformy sprzedaży biletów *online*. Każdej sprzedaży biletów online towarzyszy zapytanie o zgodę na wykorzystanie danych kontaktowych w celach marketingowych. Aby wyrazić zgodę w tym celu, klienci mogą wybrać „Nie" lub „Tak". Administrator informuje klientów o możliwości wycofania zgody. W tym celu klienci mogą bezpłatnie skontaktować się z centrum obsługi telefonicznej w dniach roboczych w godzinach 8.00–17.00. W tym przykładzie administrator nie spełnił wymogów art. 7 ust. 3 RODO. W tym przypadku wycofanie zgody wymaga połączenia telefonicznego w godzinach pracy, co jest bardziej uciążliwe niż jedno kliknięciem myszą potrzebne do wyrażenia zgody za pośrednictwem platformy sprzedaży biletów online, dostępnej 24 godziny na dobę.

116. Wymóg łatwego wycofania zgody został opisany w RODO jako niezbędny aspekt ważnej zgody. Jeżeli prawo do wycofania zgody nie spełnia wymogów RODO, wówczas stosowany przez administratora mechanizm zgody nie jest zgodny z RODO. Jak wskazano w sekcji 3.1 dotyczącej warunku *świadomej* zgody, administrator musi poinformować osobę, której dane dotyczą, o prawie do wycofania zgody jeszcze przed faktycznym wyrażeniem zgody zgodnie z art. 7 ust. 3 RODO. Ponadto w ramach obowiązku zapewnienia przejrzystości administrator musi poinformować osoby, których dane dotyczą, o sposobie korzystania z przysługujących im praw[54].

117. Co do zasady w razie wycofania zgody wszystkie operacje przetwarzania danych, które przeprowadzono w oparciu o tę zgodę przed jej wycofaniem i które były zgodne z RODO, pozostają zgodne z prawem, jednak administrator musi zaprzestać przetwarzania tych danych. Jeżeli nie ma innej zgodnej z prawem podstawy przetwarzania danych (np. dalsze przechowywanie), administrator powinien je usunąć[55].

118. Jak wskazano wcześniej w niniejszych wytycznych, bardzo ważne jest, aby administratorzy oceniali faktyczne cele przetwarzania danych i zgodne z prawem podstawy takiego przetwarzania przed zgromadzeniem danych. Przedsiębiorstwa często potrzebują danych osobowych do różnych celów, a przetwarzanie opiera się na więcej niż jednej zgodnej z prawem podstawie, np. przetwarzanie danych klientów może odbywać się na podstawie umowy i zgody. Oznacza to, że wycofanie zgody nie jest jednoznaczne z obowiązkiem usunięcia danych przetwarzanych w określonym celu wynikającym z umowy z osobą, której dane dotyczą. W związku z tym administratorzy powinni od początku jasno określić, jaki jest cel przetwarzania konkretnych danych i jaka jest zgodna z prawem podstawa takiego przetwarzania.

119. Po wycofaniu zgody administratorzy mają obowiązek usunąć dane, które przetwarzano na jej podstawie, zakładając, że nie ma innych celów uzasadniających dalsze ich przechowywanie[56]. Poza tą sytuacją, którą przewidziano w art. 17 ust. 1 lit. b), konkretna osoba, której dane dotyczą, może zażądać usunięcia innych dotyczących jej danych, które są przetwarzanie na innej zgodnej z prawem podstawie, np. na podstawie art. 6 ust. 1 lit. b)[57]. Administratorzy mają obowiązek ocenić, czy dalsze przetwarzanie odnośnych danych jest właściwe, nawet jeżeli osoba, której dane dotyczą, nie zażądała ich usunięcia[58].

120. Jeżeli osoba, której dane dotyczą, wycofuje swoją zgodę, a administrator chce w dalszym ciągu przetwarzać dane osobowe na innej zgodnej z prawem podstawie, nie może on przejść ze zgody (która zostaje wycofana) na inną zgodną z prawem podstawę bez informowania o tym zainteresowanych osób. Osoba, której dane dotyczą, powinna być informowana o każdej zmianie zgodnej z prawem podstawy przetwarzania zgodnie z wymogami w zakresie informacji określonymi w art. 13 i 14 i zgodnie z ogólną zasadą przejrzystości.

6 ZALEŻNOŚĆ MIĘDZY ZGODĄ A INNYMI ZGODNYMI Z PRAWEM PODSTAWAMI, O KTÓRYCH MOWA W ART. 6 RODO

121. W art. 6 przewidziano warunki zgodnego z prawem przetwarzania danych osobowych i opisano sześć zgodnych z prawem podstaw, na których administrator może się opierać. Zastosowanie jednej z tych sześciu podstaw musi zostać ustalone przed przetwarzaniem i w odniesieniu do określonego celu[59].

122. W tym miejscu należy wspomnieć, że jeżeli administrator postanowi opierać się na zgodzie w odniesieniu do dowolnej części przetwarzania, musi być gotowy przestrzegać tego wyboru i zaprzestać danej części przetwarzania, jeżeli dana osoba wycofa zgodę. Poinformowanie, że dane będą przetwarzane na podstawie zgody, podczas gdy administrator w praktyce opiera się na innej zgodnej z prawem podstawie, byłoby zdecydowanie nieuczciwe względem zainteresowanych osób.

123. Innymi słowy, administrator nie może zastąpić zgody innymi zgodnymi z prawem podstawami. Na przykład nie można stosować uzasadnionego interesu z mocą wsteczną jako podstawy uzasadniającej przetwarzanie danych w sytuacji powstania wątpliwości co do ważności zgody. Ze względu na wymóg ujawnienia zgodnej z prawem podstawy, na której opiera się administrator w momencie gromadzenia danych osobowych, administratorzy muszą określić zgodną z prawem podstawę, która będzie miała zastosowanie, jeszcze przed zebraniem danych.

[53] Zob. także opinia GR29 4/2010 na temat europejskiego kodeksu postępowania Europejskiej Federacji Stowarzyszeń Marketingu Bezpośredniego (FEDMA) w sprawie ochrony danych osobowych wykorzystywanych w marketingu bezpośrednim (WP 174) oraz opinia w sprawie wykorzystywania danych dotyczących lokalizacji w celu świadczenia usług tworzących wartość dodaną (WP 115).

[54] Zgodnie z motywem 39 RODO, który odnosi się do art. 13 i 14 tego rozporządzenia, „osobom fizycznym należy uświadomić ryzyka, zasady, zabezpieczenia i prawa związane z przetwarzaniem danych osobowych oraz sposoby wykonywania praw przysługujących im w związku z takim przetwarzaniem".

[55] Zob. art. 17 ust. 1 lit. b) i ust. 3 RODO.

[56] Wówczas pozostałe cele uzasadniające przetwarzanie muszą opierać się na odrębnej podstawie prawnej. Nie oznacza to, że administrator może zastąpić zgodę inną zgodną z prawą podstawą; zob. sekcja 6 poniżej.

[57] Zob. art. 17, w tym wyjątki, które mogą mieć zastosowanie, i motyw 65 RODO.

[58] Zob. także art. 5 ust. 1 lit. e) RODO.

[59] Zgodnie z art. 13 ust. 1 lit. c) lub art. 14 ust. 1 lit. c) administrator musi poinformować o tym osobę, której dane dotyczą.

7 SZCZEGÓLNIE ISTOTNE OBSZARY W RODO

7.1 Dzieci (art. 8)

124. W porównaniu z obowiązującą dyrektywą RODO tworzy dodatkową warstwę ochronną w przypadku przetwarzania danych osobowych osób fizycznych wymagających szczególnego traktowania, w szczególności dzieci. W art. 8 wprowadzono dodatkowe obowiązki w celu zapewnienia zwiększonego poziomu ochrony danych dzieci w związku z usługami społeczeństwa informacyjnego. Przyczyny zwiększonej ochrony określono w motywie 38: „[...] mogą one być mniej świadome ryzyka, konsekwencji, zabezpieczeń i praw przysługujących im w związku z przetwarzaniem danych osobowych [...]". W motywie 38 określono również, że „taka szczególna ochrona powinna mieć zastosowanie przede wszystkim do wykorzystywania danych osobowych dzieci do celów marketingowych lub do tworzenia profili osobowych lub profili użytkownika oraz do zbierania danych osobowych dotyczących dzieci, gdy korzystają one z usług skierowanych bezpośrednio do nich". Wyrażenie „przede wszystkim" wskazuje, że szczególna ochrona nie ogranicza się do celów marketingowych lub tworzenia profili, ale obejmuje również szerzej zakrojone „zbieranie danych osobowych dotyczących dzieci".

125. Art. 8 ust. 1 stanowi, że jeżeli zastosowanie ma zgoda, w przypadku usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku zgodne z prawem jest przetwarzanie danych osobowych dziecka, które ukończyło 16 lat. Jeżeli dziecko nie ukończyło 16 lat, takie przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy zgodę wyraziła lub zatwierdziła osoba sprawująca władzę rodzicielską lub opiekę nad dzieckiem oraz wyłącznie w zakresie wyrażonej zgody[60]. Jeżeli chodzi o granicę wieku, jaka jest niezbędna do wyrażenia ważnej zgody, w RODO przewidziano pewną elastyczność, a państwa członkowskie mogą określić w prawie niższy wiek, jednak nie niższy niż 13 lat.

126. Jak wskazano w sekcji 3.1 na temat świadomej zgody, informacje powinny być zrozumiałe dla odbiorców, do których zwraca się administrator, przy zwróceniu szczególnej uwagi na sytuację dzieci. Aby uzyskać od dziecka „świadomą zgodę", administrator musi wyjaśnić, jak ma zamiar przetwarzać zgromadzone dane, przy użyciu języka, który jest jasny i zrozumiały dla dzieci[61]. Jeżeli zgodę ma wyrazić rodzic, wówczas może być niezbędny zestaw informacji, który umożliwi osobom dorosłym podjęcie świadomej decyzji.

127. Z powyższego wyraźnie wynika, że przepisy art. 8 mają zastosowanie wyłącznie wtedy, gdy spełnione są następujące warunki:

- przetwarzanie dotyczy usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku;[62][63]
- przetwarzanie jest oparte na zgodzie.

7.1.1 Usługi społeczeństwa informacyjnego

128. Aby określić zakres pojęcia „usługi społeczeństwa informacyjnego" w RODO, w art. 4 pkt 25 RODO odwołano się do dyrektywy 2015/1535.

129. Oceniając zakres tej definicji, EROD odnosi się również do orzecznictwa Trybunału Sprawiedliwości[64]. Trybunał Sprawiedliwości orzekł, że *usługi społeczeństwa informacyjnego* obejmują umowy i inne usługi, które są zawierane lub świadczone drogą elektroniczną. Jeżeli usługa ma dwa niezależne ekonomicznie komponenty, z których jeden występuje online, takie jak oferta i akceptacja oferty w kontekście zawarcia umowy lub informacji dotyczących produktów lub usług, w tym działań marketingowych, komponent ten jest zdefiniowany jako usługa społeczeństwa informacyjnego, a drugi komponent będący fizyczną dostawą lub dystrybucją towarów nie będzie objęty pojęciem usługi społeczeństwa informacyjnego Świadczenie usługi w trybie online wchodzi w zakres pojęcia *usługi społeczeństwa informacyjnego* określonej w art. 8 RODO.

7.1.2 Usługi oferowane bezpośrednio dziecku

130. Sformułowanie „oferowane bezpośrednio dziecku" wskazuje, że art. 8 ma zastosowanie do niektórych, lecz nie do wszystkich usług społeczeństwa informacyjnego. W tym zakresie jeżeli dostawca usług społeczeństwa informacyjnego wyraźnie poinformuje potencjalnych użytkowników, że oferuje swoją usługę wyłącznie osobom, które skończyły 18 lat, i jeżeli inne dowody nie wskazują inaczej (np. treść strony lub plany marketingowe), wówczas usługa nie zostanie uznana za „oferowaną bezpośrednio dziecku", a przepisy art. 8 nie będą miały zastosowania.

[60] Niezależnie od możliwości odstępstwa od granicy wieku w prawach państw członkowskich zob. art. 8 ust. 1.

[61] W motywie 58 RODO potwierdzono ten obowiązek, stwierdzając, że administrator powinien zapewnić, by przekazywane informacje były zrozumiałe dla dzieci.

[62] Zgodnie z art. 4 pkt 25 RODO usługa społeczeństwa informacyjnego oznacza usługę w rozumieniu art. 1 ust. 1 lit. b) dyrektywy 2015/1535: „b) »usługa« oznacza każdą usługę społeczeństwa informacyjnego, to znaczy każdą usługę normalnie świadczoną za wynagrodzeniem, na odległość, drogą elektroniczną i na indywidualne żądanie odbiorcy usług. Do celów niniejszej definicji: (i) »na odległość« oznacza, że usługa świadczona jest bez równoczesnej obecności stron; (ii) »drogą elektroniczną« oznacza, iż usługa jest wysyłana i odbierana w miejscu przeznaczenia za pomocą sprzętu elektronicznego do przetwarzania (włącznie z kompresją cyfrową) oraz przechowywania danych, i która jest całkowicie przesyłana, kierowana i otrzymywana za pomocą kabla, fal radiowych, środków optycznych lub innych środków elektromagnetycznych; (iii) »na indywidualne żądanie odbiorcy usług« oznacza, że usługa świadczona jest poprzez przesyłanie danych na indywidualne żądanie". W załączniku I do tej dyrektywy podano orientacyjny wykaz usług nieobjętych niniejszą definicją. Zob. także motyw 18 dyrektywy 2000/31.

[63] Zgodnie z art. 1 konwencji ONZ o prawach dziecka „[...] »dziecko« oznacza każdą istotę ludzką w wieku poniżej osiemnastu lat, chyba że zgodnie z prawem odnoszącym się do dziecka uzyska ono wcześniej pełnoletność", zob. rezolucja Zgromadzenia Ogólnego ONZ 44/25 z dnia 20 listopada 1989 r. (konwencja o prawach dziecka).

[64] Zob. wyrok Trybunału Sprawiedliwości z dnia 2 grudnia 2010 r., C-108/09 (Ker-Optika), pkt 22 i 28. W odniesieniu do usług mieszanych EROD odwołuje się również do pkt 40 wyroku w sprawie C-434/15 (Asociación Profesional Elite Taxi przeciwko Uber Systems Spain S.L), w którym stwierdzono, że usługi społeczeństwa informacyjnego stanowiącej integralną część złożonej usługi, której głównym elementem nie jest usługa społeczeństwa informacyjnego (w tym przypadku jest to usługa przewozowa), nie należy kwalifikować jako „usługę społeczeństwa informacyjnego".

7.1.3 Wiek

131. RODO stanowi, że „państwa członkowskie mogą przewidzieć w swoim prawie niższą granicę wiekową, która musi wynosić co najmniej 13 lat". Administrator musi być świadomy różnic w przepisach krajowych, uwzględniając docelową grupę odbiorców jego usług. W szczególności należy zauważyć, że administrator świadczący usługę transgraniczną nie zawsze może polegać wyłącznie na zgodności z prawem państwa członkowskiego, w którym ma swoją główną jednostkę organizacyjną, ale może być zobowiązany do przestrzegania odpowiednich przepisów krajowych każdego państwa członkowskiego, w którym oferuje usługę lub usługi społeczeństwa informacyjnego. Zależy to od tego, czy państwo członkowskie wybierze – jako punkt odniesienia w prawie krajowym – miejsce głównej jednostki organizacyjnej administratora czy też miejsce zamieszkania osoby, której dane dotyczą. Państwa członkowskie, przy podejmowaniu tej decyzji, powinny brać pod uwagę przede wszystkim dobro dziecka. Grupa Robocza zachęca państwa członkowskie do poszukiwania zharmonizowanego rozwiązania w tym zakresie.

132. Świadcząc dzieciom usługi społeczeństwa informacyjnego na podstawie zgody, administratorzy powinni podjąć rozsądne starania, by zweryfikować, czy użytkownik osiągnął wiek uprawniający do wyrażenia zgody drogą elektroniczną, przy czym starania te powinny być proporcjonalne do charakteru czynności przetwarzania i związanego z nimi ryzyka.

133. Jeżeli użytkownicy oświadczą, że są w wieku uprawniającym do wyrażenia zgody drogą elektroniczną, wówczas administrator może podjąć właściwe czynności kontrolne, by zweryfikować, czy te oświadczenia są prawdziwe. Chociaż w RODO nie wskazano wyraźnie konieczności podjęcia rozsądnych starań w celu zweryfikowania wieku, jest to w sposób dorozumiany wymagane, ponieważ jeżeli dziecko wyrazi zgodę, a nie osiągnęło wystarczającego wieku, aby udzielić ważnej zgody we własnym imieniu, taka czynność sprawi, to spowoduje to niezgodność z prawem przetwarzania danych.

134. Jeżeli użytkownik oświadczy, że nie osiągnął wieku uprawniającego do wyrażenia zgody drogą cyfrową, administrator może przyjąć takie oświadczenie bez konieczności podejmowania dalszych działań kontrolnych, ale będzie musiał przejść do uzyskania zgody rodzica lub opiekuna i zweryfikować, że osoba udzielająca takiej zgody sprawuje władzę rodzicielską lub opiekę nad dzieckiem.

135. Weryfikacja wieku nie powinna prowadzić do nadmiernego przetwarzania danych. Mechanizm wybrany do weryfikacji wieku osoby, której dane dotyczą, powinien obejmować ocenę ryzyka związanego z proponowanym przetwarzaniem. W niektórych sytuacjach niskiego ryzyka właściwe może być zobowiązanie nowego abonenta usługi do ujawnienia roku urodzenia lub wypełnienia formularza, w którym oświadczy, że (nie) jest osobą małoletnią[65]. W razie wątpliwości administrator powinien przeanalizować swoje mechanizmy weryfikacji wieku w danym przypadku i rozważyć, czy niezbędne są alternatywne sposoby weryfikacji[66].

7.1.4 Zgoda udzielana przez dzieci i władza rodzicielska

136. Jeżeli chodzi o potwierdzenie przez osobę posiadającą władzę rodzicielską lub sprawującą opiekę nad dzieckiem, w RODO nie wskazano konkretnych praktycznych sposobów na uzyskanie zgody rodzica lub ustalenie, że dana osoba jest uprawniona do podjęcia takiej czynności[67]. W związku z tym EROD zaleca przyjęcie proporcjonalnego podejścia zgodnie z art. 8 ust. 2 i art. 5 ust. 1 lit. c) RODO (minimalizacja danych). Proporcjonalne podejście mogłoby polegać na dążeniu do uzyskania ograniczonej ilości informacji, takich jak dane kontaktowe rodzica lub opiekuna.

137. Racjonalność działań podejmowanych w celu weryfikacji, czy dany użytkownik osiągnął odpowiedni wiek do samodzielnego wyrażenia zgody oraz czy osoba wyrażająca zgodę w imieniu dziecka sprawuje władzę rodzicielską lub opiekę nad dzieckiem, może zależeć od ryzyka związanego z przetwarzaniem oraz od dostępnej technologii. W sytuacjach niskiego ryzyka może wystarczyć weryfikacja posiadania władzy rodzicielskiej za pośrednictwem poczty elektronicznej. W sytuacjach wysokiego ryzyka właściwe może być natomiast poproszenie o więcej dowodów, tak by administrator był w stanie zweryfikować i przechowywać informacje zgodnie z art. 7 ust. 1 RODO[68]. Usługi zaufanej strony trzeciej w zakresie weryfikacji mogą być rozwiązaniami ograniczającymi do minimum ilość danych osobowych, które muszą zostać przetworzone przez samego administratora danych.

138. Przykład 23: Internetowa platforma gier chce się upewnić, że małoletni konsumenci subskrybują jej usługi wyłącznie za zgodą swoich rodziców lub opiekunów. Administrator podejmuje następujące kroki:

139. Krok 1: prosi użytkownika o informację, czy osiągnął on wiek 16 lat (lub inny wiek uprawniający do wyrażenia zgody drogą elektroniczną). Jeżeli użytkownik oświadczy, że nie osiągnął wieku uprawniającego do wyrażenia zgody drogą elektroniczną:

140. Krok 2: platforma informuje dziecko, że rodzic lub opiekun musi wcześniej wyrazić zgodę lub zezwolić na przetwarzanie danych dziecka, zanim nastąpi świadczenie usługi dziecku. Użytkownik jest proszony o podanie adresu e-mail rodzica lub opiekuna.

141. Krok 3: platforma kontaktuje się z rodzicem lub opiekunem i za pomocą poczty elektronicznej uzyskuje jego zgodę na przetwarzanie danych oraz podejmuje rozsądne kroki w celu upewnienia się, że dana osoba dorosła sprawuje władzę rodzicielską.

142. Krok 4: w przypadku skarg platforma podejmuje dodatkowe działania w celu weryfikacji wieku abonenta.

143. Jeżeli platforma spełniła pozostałe wymogi dotyczące zgody, może ona spełnić dodatkowe kryteria wymienione w art. 8 RODO, podejmując te kroki.

144. Przykład ten pokazuje, że administrator danych jest w stanie wykazać, że podjęto rozsądne działania, aby upewnić się, że udzielona została ważna zgoda w odniesieniu do usług świadczonych dziecku. W art. 8 ust. 2 w szczególności dodano, że „administrator, uwzględniając dostępną technologię, podejmuje rozsądne starania, by zweryfikować, czy osoba sprawująca władzę rodzicielską lub opiekę nad dzieckiem wyraziła zgodę lub ją zaaprobowała".

[65] Chociaż nie zawsze to rozwiązanie jest pozbawione wad, jest to przykład tego, jak można dopełnić wymogu wynikającego z tego przepisu.

[66] Zob. opinia GR29 5/2009 w sprawie portali społecznościowych (WP 163).

[67] GR29 zauważa, że nie zawsze osoba sprawująca władzę rodzicielską lub opiekę nad dzieckiem jest rodzicem biologicznym dziecka i że władzę rodzicielską może sprawować wiele osób, w tym osoby prawne i fizyczne.

[68] Przykładowo rodzic lub opiekun może zostać poproszony o dokonanie płatności w wysokości 0,01 EUR na rzecz administratora za pomocą przelewu bankowego, w tym o krótkie potwierdzenie w opisie transakcji, że posiadacz rachunku bankowego sprawuje władzę rodzicielską lub opiekę nad użytkownikiem. W stosownych przypadkach należy zapewnić alternatywną metodę weryfikacji, aby zapobiec nieuzasadnionemu dyskryminacyjnemu traktowaniu osób, które nie posiadają rachunku bankowego.

145. Do administratora należy ustalenie, jakie środki są odpowiednie w konkretnym przypadku. Co do zasady administratorzy powinni unikać rozwiązań w zakresie weryfikacji, które same w sobie wymagają nadmiernego zbierania danych osobowych.

146. EROD przyznaje, że w niektórych przypadkach weryfikacja jest trudna, np. kiedy dzieci udzielające zgody nie pozostawiły jeszcze swojego śladu cyfrowego lub wówczas, gdy nie jest łatwo sprawdzić, czy dana osoba sprawuje władzę rodzicielską. Można to uwzględnić przy podejmowaniu decyzji o tym, które starania są rozsądne, ale oczekuje się również, że administratorzy będą poddawać swoje procesy i dostępną technologię ciągłym przeglądom.

147. W odniesieniu do autonomii osoby, której dane dotyczą, w zakresie udzielania zgody na przetwarzanie danych osobowych i sprawowania przez nią pełnej kontroli nad tym procesem zgoda osoby posiadającej władzę rodzicielską na przetwarzanie danych osobowych dziecka może zostać potwierdzona, zmieniona lub wycofana z chwilą osiągnięcia przez osobę, której dane dotyczą, wieku uprawniającego do wyrażenia zgody drogą elektroniczną.

148. W praktyce oznacza to, że jeżeli dziecko nie podejmuje żadnych działań, zgoda udzielona przez osobę sprawującą władzę rodzicielską lub opiekę nad dzieckiem lub pozwolenie na przetwarzanie danych osobowych udzielone przez osobę sprawującą władzę lub opiekę rodzicielską nad dzieckiem przed osiągnięciem przez dziecko wieku uprawniającego do wyrażenia zgody drogą elektroniczną pozostaje ważną podstawą przetwarzania danych.

149. Po osiągnięciu wieku uprawniającego do wyrażenia zgody drogą elektroniczną dziecko będzie mogło samodzielnie wycofać zgodę zgodnie z art. 7 ust. 3. Zgodnie z zasadami uczciwości i odpowiedzialności administrator musi poinformować dziecko o takiej możliwości[69].

150. Należy podkreślić, że zgodnie z motywem 38 zgoda rodzica lub opiekuna nie jest wymagana w przypadku usług profilaktycznych lub doradczych oferowanych bezpośrednio dziecku. Na przykład świadczenie dziecku usług z zakresu ochrony dziecka za pośrednictwem czatu internetowego nie wymaga wcześniejszej zgody rodzica.

151. Ponadto w RODO określono, że przepisy dotyczące wymogów udzielania zgody przez rodziców lub opiekunów w odniesieniu do małoletnich nie powinny wpływać na „ogólne przepisy prawa umów państw członkowskich, takie jak przepisy o ważności, zawieraniu lub skutkach umowy wobec dziecka". W związku z tym wymogi w zakresie ważnej zgody na wykorzystywanie danych dotyczących dzieci są częścią ram prawnych, które należy postrzegać jako odrębne od krajowego prawa umów. W niniejszych wytycznych nie poruszono zatem kwestii tego, czy małoletni mogą zgodnie z prawem zawierać umowy przez internet. Oba systemy prawne mogą mieć jednocześnie zastosowanie, a zakres zastosowania RODO nie obejmuje ujednolicenia przepisów krajowych prawa umów.

[69] Ponadto osoba, której dane dotyczą, powinna zdawać sobie sprawę z posiadania prawa do bycia zapomnianym zgodnie z art. 17, co jest szczególnie istotne w przypadku zgody udzielonej, kiedy osoba, której dane dotyczą, była jeszcze dzieckiem; zob. motyw 63.

7.2 Badania naukowe

152. Definicja celów badań naukowych ma istotne konsekwencje dla szeregu czynności przetwarzania danych, które może podejmować administrator. Termin „badania naukowe" nie jest zdefiniowany w RODO. Motyw 159 stanowi, że „(...) W niniejszym rozporządzeniu przetwarzanie danych osobowych do celów badań naukowych należy interpretować szeroko (...)", EROD uważa jednak, że pojęcia tego nie można rozciągać poza jego powszechne znaczenie, i jest zdania, że w tym kontekście „badania naukowe" oznaczają projekt badawczy zorganizowany zgodnie z odpowiednimi normami metodycznymi i etycznymi w danym sektorze oraz zgodnie z dobrymi praktykami.

153. Jeżeli podstawą prawną do przeprowadzenia badań zgodnie z RODO jest zgoda, należy odróżnić taką zgodę na wykorzystywanie danych osobowych od innych wymogów w zakresie zgody, które stanowią normę etyczną lub obowiązek proceduralny. Przykłady takich obowiązków proceduralnych, w których przetwarzanie odbywa się na innej podstawie prawnej niż zgoda, znajdują się w rozporządzeniu w sprawie badań klinicznych. W kontekście prawa w dziedzinie ochrony danych taką formę zgody można traktować jako dodatkowe zabezpieczenie[70]. Jednocześnie w odniesieniu do przetwarzania danych do celów badań RODO nie ogranicza zastosowania art. 6 wyłącznie do zgody. Możliwe są inne podstawy prawne, takie jak art. 6 ust. 1 lit. e) lub f), jeżeli istnieją właściwe zabezpieczenia, np. wymogi przewidziane w art. 89 ust. 1, a przetwarzanie jest uczciwe, zgodne z prawem, przejrzyste oraz zgodne z normami w zakresie minimalizacji danych i prawami poszczególnych osób[71]. Dotyczy to również szczególnych kategorii danych zgodnie z odstępstwem, o którym mowa w art. 9 ust. 2 lit. j)[72].

154. Wydaje się, że w motywie 33 wprowadzono pewną elastyczność co do stopnia specjalizacji i szczegółowości zgody w kontekście badań naukowych. Motyw 33 stanowi, że: „w momencie zbierania danych często nie da się w pełni zidentyfikować celu przetwarzania danych osobowych na potrzeby badań naukowych. Dlatego osoby, których dane dotyczą, powinny móc wyrazić zgodę na niektóre obszary badań naukowych, o ile badania te są zgodne z uznanymi normami etycznymi w zakresie badań naukowych. Osoby, których dane dotyczą, powinny móc wyrazić zgodę tylko na niektóre obszary badań lub elementy projektów badawczych, o ile umożliwia to zamierzony cel".

155. Po pierwsze należy zauważyć, że motyw 33 nie uchyla obowiązków dotyczących wymogu uzyskania konkretnej zgody. Oznacza to, że w projektach badań naukowych można zasadniczo wykorzystywać dane osobowe na podstawie zgody tylko wtedy, gdy właściwie opisano ich cel. W przypadku projektów badań naukowych, w odniesieniu do których nie można z góry określić szczegółowo celów przetwarzania danych, w motywie 33 przewidziano wyjątek, zgodnie z którym cel można opisać bardziej ogólnie.

156. Mając na uwadze rygorystyczne warunki, które ustanowiono w art. 9 RODO w odniesieniu do przetwarzania szczególnych kategorii danych, EROD zauważa, że w przypadku przetwarzania szczególnych kategorii danych w oparciu o wyraźną zgodę zastosowanie elastycznego podejścia

[70] Zob. także motyw 161 RODO.

[71] Przepisy art. 6 ust. 1 lit. c) mogą mieć zastosowanie również do części operacji przetwarzania, które są szczególnie wymagane przez prawo, np. do zbierania wiarygodnych i solidnych danych zgodnie z protokołem zatwierdzonym przez dane państwo członkowskie na podstawie rozporządzenia w sprawie badań klinicznych.

[72] Określone testy produktów leczniczych mogą odbywać się zgodnie z przepisami unijnymi lub prawem krajowym na podstawie art. 9 ust. 2 lit. i).

zgodnie z motywem 33 powinno być interpretowane bardziej zawężająco i wymaga wysokiego stopnia kontroli.

157. W ujęciu ogólnym RODO nie może być interpretowane w sposób umożliwiający administratorowi obejście zasadniczej zasady szczegółowego określenia celów, w odniesieniu do których prosi się o zgodę osoby, której dane dotyczą.

158. Jeżeli nie można w pełni określić celów badań, administrator musi szukać innych sposobów zapewnienia, aby jak najlepiej zrealizować istotę wymogów w zakresie zgody, np. umożliwić osobom, których dane dotyczą, udzielenie zgody na dany cel badania określony bardziej ogólnie oraz umożliwić realizację poszczególnych etapów projektu badawczego, które znane są już na początku. W miarę postępu badań przed rozpoczęciem kolejnego etapu można uzyskać zgodę na następne etapy projektu. Taka zgoda nadal powinna być jednak zgodna z mającymi zastosowanie normami etycznymi w zakresie badań naukowych.

159. Ponadto administrator może ustanowić w takich przypadkach dodatkowe zabezpieczenia. Przykładowo w art. 89 ust. 1 podkreślono konieczność ustanowienia zabezpieczeń w zakresie czynności przetwarzania danych do celów badań naukowych lub historycznych lub do celów statystycznych. Cele te powinny podlegać „odpowiednim zabezpieczeniom dla praw i wolności osoby, której dane dotyczą, zgodnie z niniejszym rozporządzeniem". Wśród możliwych zabezpieczeń wymieniono minimalizację danych, anonimizację i zapewnienie bezpieczeństwa danych[73]. Anonimizacja jest preferowanym rozwiązaniem na etapach, gdy cel badania można osiągnąć bez przetwarzania danych osobowych.

160. Przejrzystość jest dodatkowym zabezpieczeniem, jeżeli okoliczności badania nie pozwalają na uzyskanie konkretnej zgody. Aby zrekompensować brak uszczegółowienia celu, administratorzy mogą regularnie podawać informacje na temat rozwoju celu w miarę postępu projektu badawczego, tak aby z czasem zgoda była tak konkretna, jak to tylko możliwe. W ten sposób osoba, której dane dotyczą, ma przynajmniej podstawowy obraz aktualnej sytuacji, dzięki czemu może ocenić, czy np. powinna skorzystać z prawa cofnięcia zgody na podstawie art. 7 ust. 3[74].

[73] Zob. np. motyw 156. Przetwarzanie danych osobowych do celów naukowych powinno też być zgodne z innymi odpowiednimi przepisami, takimi jak przepisy o próbach klinicznych; zob. motyw 156, w którym jest mowa o rozporządzeniu Parlamentu Europejskiego i Rady (UE) nr 536/2014 z dnia 16 kwietnia 2014 r. w sprawie badań klinicznych produktów leczniczych stosowanych u ludzi. Zob. także opinia GR29 15/2011 w sprawie definicji zgody (WP 187), s. 7: „Ponadto uzyskanie zgody nie zwalnia administratora danych z obowiązków na mocy art. 6 związanych z rzetelnością, koniecznością i proporcjonalnością, jak też jakością danych. Na przykład nawet jeżeli użytkownik wyraził zgodę na przetwarzanie danych osobowych, nie czyni to legalnym gromadzenia danych nadmiernych w stosunku do określonego celu. (...) Co do zasady, zgody nie należy uważać za odstępstwo od pozostałych zasad ochrony danych, lecz za zabezpieczenie. Jest ona przede wszystkim podstawą do zapewnienia zgodności z prawem i nie zwalnia z obowiązku stosowania innych zasad".

[74] Istotne mogą być również inne środki na rzecz przejrzystości. Jeżeli administratorzy przetwarzają dane do celów naukowych, a przekazanie wszystkich informacji na początku nie jest możliwe, mogą wyznaczyć konkretną osobę do kontaktu dla osób, których dane dotyczą, aby mogły one kierować do niej swoje pytania.

161. Brak uszczegółowienia celu można zrekompensować również poprzez udostępnienie do wglądu kompleksowego planu badawczego osobom, których dane dotyczą, zanim wyrażą one zgodę[75]. W takim planie badawczym należy jak najbardziej szczegółowo określić badane zagadnienia i przewidywane metody pracy. Plan badawczy może również pomóc w zapewnieniu zgodności z przepisami art. 7 ust. 1, ponieważ aby móc udowodnić, że uzyskana zgoda jest ważna, administratorzy muszą wskazać, jakie informacje były dostępne dla osób, których dane dotyczą, w momencie udzielania przez nich zgody.

162. Należy przypomnieć, że jeżeli zgoda jest stosowana jako zgodna z prawem podstawa przetwarzania, osoba, której dane dotyczą, musi mieć możliwość wycofania tej zgody. EROD zauważa, że wycofanie zgody może podważyć te rodzaje badań naukowych, które wymagają danych, które można powiązać z poszczególnymi osobami; w RODO jednak wyraźnie przewidziano możliwość wycofania takiej zgody, a administratorzy muszą odpowiednio reagować na takie działanie – w rozporządzeniu nie przewidziano odstępstwa od tego wymogu w przypadku badań naukowych. Jeśli administrator otrzyma żądanie wycofania zgody, musi zasadniczo bezzwłocznie usunąć dane osobowe, jeżeli chce w dalszym ciągu wykorzystywać dane do celów badania[76].

7.3 Prawa osób, których dane dotyczą

163. Jeżeli czynność przetwarzania danych opiera się na zgodzie osoby, której dane dotyczą, będzie to miało wpływ na prawa tej osoby. Osoby, której dane dotyczą, mogą mieć prawo do przenoszenia danych (art. 20), gdy przetwarzanie odbywa się w oparciu o zgodę. Natomiast prawo do sprzeciwu (art. 21) nie ma zastosowania, jeżeli przetwarzanie odbywa się w oparciu o zgodę, jednak prawo do wycofania zgody w dowolnym momencie może wywołać podobne skutki.

164. Zgodnie z art. 16–20 RODO (jeżeli przetwarzanie danych odbywa się w oparciu o zgodę) osoby, których dane dotyczą, mają prawo do usunięcia danych, jeżeli zgoda została wycofana, oraz prawo do ograniczenia przetwarzania, sprostowania danych i dostępu do danych[77].

8 ZGODA UZYSKANA NA MOCY DYREKTYWY 95/46/WE

165. Od administratorów, którzy obecnie przetwarzają dane w oparciu o zgodę zgodnie z krajowym prawem w dziedzinie ochrony danych, nie wymaga się automatycznie całkowitego odświeżenia wszystkich istniejących stosunków w zakresie zgody z osobami, których dane dotyczą, w ramach przygotowań do wdrożenia RODO. Zgoda, którą uzyskano do tego czasu, pozostaje ważna w zakresie, w jakim jest ona zgodna z warunkami określonymi w RODO.

166. Ważne jest, aby przed dniem 25 maja 2018 r. administratorzy dokonali szczegółowego przeglądu obecnych procesów operacyjnych i rejestrów, aby zapewnić zgodność istniejących treści z normami

[75] Możliwość taką przewidziano w art. 14 ust. 1 obowiązującej fińskiej ustawy o danych osobowych (Henkilötietolaki, 523/1999).

[76] Zob. także opinia GR29 05/2014 w sprawie technik anonimizacji (WP 216).

[77] W przypadkach, w których zgodnie z art. 18 RODO niektóre czynności przetwarzania danych zostają ograniczone, usunięcie takich ograniczeń może wymagać zgody osoby, której dane dotyczą.

określonymi w RODO (zob. motyw 171 RODO)[78]. W praktyce RODO podnosi poprzeczkę w odniesieniu do wdrażania mechanizmów zgody i wprowadzono szereg nowych wymogów, których spełnienie narzuca administratorom konieczność zmiany mechanizmów zgody, a nie tylko przeredagowania polityk prywatności[79].

167. Na przykład ponieważ zgodnie z RODO administrator musi być wstanie wykazać, że uzyskał ważną zgodę, wszelkie domniemane zgody, w przypadku których nie przechowuje się żadnych odniesień, automatycznie nie będą spełniać standardu zgody na mocy RODO i będą musiały zostać odnowione. Podobnie ponieważ RODO wymaga „oświadczenia lub wyraźnego działania potwierdzającego", wszelkie domniemane zgody, które oparto na bardziej dorozumianej formie działania ze strony osoby, której dane dotyczą (np. domyślnie zaznaczone okienko zgody), również nie będą spełniać standardu normy na mocy RODO.

168. Ponadto konieczny może być przegląd czynności i systemów informatycznych, aby móc wykazać uzyskanie zgody lub umożliwić bardziej szczegółowe okazanie woli przez osoby, których dane dotyczą. Ponadto należy zapewnić łatwy dostęp do mechanizmów wycofania zgody przez osoby, których dane dotyczą, oraz informacje na temat tego, jak wycofać zgodę. Jeżeli istniejące procedury uzyskiwania zgody i zarządzania zgodą nie spełniają standardów RODO, administratorzy będą musieli uzyskać nową zgodę zgodną z RODO.

169. Z drugiej strony ponieważ nie wszystkie elementy przewidziane w art. 13 i 14 muszą być zawsze występować jako warunek świadomej zgody, rozszerzone obowiązki w zakresie informacji, o których mowa w RODO, niekoniecznie naruszają ciągłość zgody wyrażonej przed wejściem RODO w życie (zob. s. 15 powyżej). W dyrektywie 95/46/WE nie przewidziano obowiązku informowania osób, których dane dotyczą, o podstawach, na których prowadzono przetwarzanie.

170. Jeżeli administrator ustali, że zgoda uzyskana wcześniej na podstawie dawnych przepisów nie będzie spełniać standardu zgody na mocy RODO, wówczas musi on podjąć działania w celu zapewnienia zgodności z tymi standardami, np. przez odnowienie zgody w sposób zgodny z RODO. W RODO nie przewidziano możliwości zastąpienia jednej zgodnej z prawem podstawą inną podstawą. Jeżeli administrator nie jest w stanie odnowić zgody w sposób zgodny z RODO i nie jest także w stanie osiągnąć zgodności z RODO przez oparcie przetwarzania danych na innej zgodnej z prawem podstawie przy jednoczesnym zapewnieniu, by dalsze przetwarzanie odbywało się w sposób uczciwy i odpowiedzialny (przy czym taka niemożliwość osiągnięcia zgodności jest przypadkiem jednorazowym), musi zaprzestać czynności przetwarzania. W każdym przypadku administrator musi przestrzegać zasad zgodnego z prawem, uczciwego i przejrzystego przetwarzania danych.

[78] Motyw 171 RODO stanowi, że: „Niniejszym rozporządzeniem należy uchylić dyrektywę 95/46/WE. Przetwarzanie, które w dniu rozpoczęcia stosowania niniejszego rozporządzenia już się toczy, powinno w terminie dwóch lat od wejścia niniejszego rozporządzenia w życie zostać dostosowane do jego przepisów. Jeżeli przetwarzanie ma za podstawę zgodę w myśl dyrektywy 95/46/WE, osoba, której dane dotyczą, nie musi ponownie wyrażać zgody, jeżeli pierwotny sposób jej wyrażenia odpowiada warunkom niniejszego rozporządzenia; dzięki temu administrator może kontynuować przetwarzanie po dacie rozpoczęcia stosowania niniejszego rozporządzenia. Decyzje przyjęte przez Komisję oraz zezwolenia wydane przez organy nadzorcze na podstawie dyrektywy 95/46/WE pozostają w mocy do czasu ich zmiany, zastąpienia lub uchylenia".

[79] Jak wskazano we wprowadzeniu, w RODO jeszcze bardziej sprecyzowano i uszczegółowiono wymogi dotyczące uzyskania ważnej zgody oraz wykazania jej wyrażenia. Wiele nowych wymogów opiera się na opinii 15/2011 w sprawie definicji zgody.



Wytyczne 04/2020 w sprawie wykorzystywania danych o lokalizacji oraz narzędzi służących ustalaniu kontaktów zakaźnych w kontekście pandemii COVID-19

Przyjęte 21 kwietnia 2020 r.

Historia wersji

Wersja 1.1	5 maja 2020 r.	Drobne korekty
Wersja 1.0	21 kwietnia 2020 r.	Przyjęcie wytycznych

Spis treści

Spis treści ... 3
1 Wprowadzenie i kontekst ... 4
2 Wykorzystywanie danych o lokalizacji ... 6
2.1 Źródła danych o lokalizacji ... 6
2.2 Koncentracja na wykorzystywaniu zanonimizowanych danych o lokalizacji ... 6
3 Aplikacje służące do ustalania kontaktów zakaźnych ... 8
3.1 Ogólna analiza prawna ... 8
3.2 Zalecenia i wymagania funkcjonalne ... 10
4 Podsumowanie ... 12
Załącznik – Aplikacje służące do ustalania kontaktów zakaźnych Przewodnik analityczny ... 13

Europejska Rada Ochrony Danych,

uwzględniając art. 70 ust. 1 lit. e) rozporządzenia Parlamentu Europejskiego i Rady 2016/679/UE z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (zwanego dalej „RODO"),

uwzględniając Porozumienie EOG, w szczególności załącznik XI i protokół 37 tegoż, w kształcie zmienionym decyzją Wspólnego Komitetu EOG nr 154/2018 z dnia 6 lipca 2018 r.[1],

uwzględniając art. 12 i 22 swojego regulaminu wewnętrznego,

PRZYJĘŁA NASTĘPUJĄCE WYTYCZNE:

1 WPROWADZENIE I KONTEKST

1 W odpowiedzi na pandemię COVID-19 rządy oraz podmioty prywatne skłaniają się ku rozwiązaniom opartym na danych, co budzi liczne obawy dotyczące prywatności.

2 EROD podkreśla, że ramy prawne ochrony danych opracowano z myślą o tym, by były elastyczne, dzięki czemu możliwa jest skuteczna reakcja, która pozwoli zarówno ograniczyć pandemię, jak i chronić podstawowe prawa i wolności człowieka.

3 EROD jest przekonana, że w sytuacji, gdy przetwarzanie danych osobowych jest konieczne, by zaradzić pandemii COVID-19, ochrona danych osobowych jest niezbędna do budowania zaufania i tworzenia warunków społecznej akceptacji dla każdego rozwiązania, a tym samym do zagwarantowania skuteczności tych środków. Ponieważ wirus nie zna granic, korzystne wydaje się opracowanie wspólnego europejskiego podejścia w odpowiedzi na obecny kryzys lub co najmniej wdrożenie ram interoperacyjnych.

4 Co do zasady EROD jest zdania, że dane oraz technologia wykorzystywane w celu zwalczania COVID-19 powinny być używane raczej do wzmacniania pozycji osób, a nie w celu ich kontrolowania, piętnowania lub uciskania. Ponadto, podczas gdy dane i technologia mogą stanowić istotne narzędzia, mają one właściwe sobie ograniczenia i mogą jedynie zwiększyć skuteczność innych środków dotyczących zdrowia publicznego. Środki przyjmowane przez państwa członkowskie lub instytucje Unii, dotyczące przetwarzania danych osobowych w celu zwalczania pandemii COVID-19, muszą opierać się na ogólnych zasadach skuteczności, niezbędności i proporcjonalności.

5 W niniejszych wytycznych doprecyzowano warunki i zasady proporcjonalnego wykorzystania danych o lokalizacji oraz narzędzi służących ustalaniu kontaktów zakaźnych do osiągnięcia dwóch szczegółowych celów, którymi są:

- wykorzystywanie danych o lokalizacji w celu wspierania reakcji na pandemię przez tworzenie modelu rozprzestrzeniania się wirusa, służącego ocenie skuteczności środków izolacji;
- ustalanie kontaktów zakaźnych w celu informowania poszczególnych osób o tym, że znalazły się w pobliżu osoby, w przypadku której zostanie ostatecznie potwierdzone, że jest nosicielem wirusa, aby przerywać łańcuchy zakażeń na możliwie jak najwcześniejszym etapie.

6 Skuteczność wkładu aplikacji służących do ustalania kontaktów zakaźnych w kontrolowanie pandemii zależy od wielu czynników (np. od odsetka ludzi, którzy będą potrzebowali taką aplikację zainstalować; definicji „kontaktu", jeżeli chodzi o bliskość i czas trwania). Ponadto takie aplikacje muszą być elementem kompleksowej strategii zdrowia publicznego, mającej na celu zwalczanie pandemii, obejmującej m.in. badania i dalsze ustalanie kontaktów zakaźnych tradycyjnymi metodami, by rozwiać wszelkie wątpliwości. Wdrożeniu takich aplikacji powinny towarzyszyć środki wspierające mające zapewnić, aby informacje przekazywane użytkownikom były rozpatrywane w szerszym kontekście oraz aby ostrzeżenia były użyteczne dla systemu zdrowia publicznego. W przeciwnym razie aplikacje te nie będą w pełni skuteczne.

7 EROD podkreśla, że zarówno RODO, jak i dyrektywa 2002/58/WE (zwana dalej „dyrektywą") zawierają przepisy szczegółowe dopuszczające wykorzystywanie danych anonimowych lub danych osobowych w celu wspierania organów publicznych i innych podmiotów na szczeblu krajowym i unijnym w monitorowaniu i ograniczaniu rozprzestrzeniania się wirusa SARS-CoV-2[2].

8 W tym względzie EROD zajęła już stanowisko, twierdząc, że korzystanie z aplikacji służących do ustalania kontaktów zakaźnych powinno być dobrowolne i nie powinno polegać na śledzeniu poszczególnych przemieszczeń, lecz raczej powinno bazować na informacjach na temat bliskości dotyczących użytkowników[3].

1 Odniesienia do „państw członkowskich" zawarte w niniejszym dokumencie należy rozumieć jako odniesienia do „państw członkowskich EOG".

[2] Zob. poprzednie oświadczenie EROD w sprawie pandemii COVID-19.

[3] https://edpb.europa.eu/sites/edpb/files/files/file1/edpbletterecadvisecodiv-appguidance_final.pdf

2 WYKORZYSTYWANIE DANYCH O LOKALIZACJI

2.1 Źródła danych o lokalizacji

9 Istnieją dwa główne źródła danych o lokalizacji dostępne do celów tworzenia modeli rozprzestrzeniania się wirusa oraz ogólnej skuteczności środków izolacji:
- dane o lokalizacji gromadzone przez dostawców usług łączności elektronicznej (takich jak operatorzy usług telefonii komórkowej) w trakcie świadczenia usług oraz
- dane o lokalizacji gromadzone przez aplikacje podmiotów świadczących usługi społeczeństwa informacyjnego, których funkcje wymagają wykorzystania takich danych (np. nawigacja, usługi transportowe itp.).

10 EROD przypomina, że dane o lokalizacji[4] uzyskane od dostawców usług łączności elektronicznej mogą być przetwarzane wyłącznie w zakresie dopuszczonym w art. 6 i 9 dyrektywy. Oznacza to, że dane te mogą być przekazywane władzom lub innym osobom trzecim wyłącznie wówczas, gdy zostały zanonimizowane przez usługodawcę lub – w przypadku danych wskazujących położenie geograficzne terminala niebędących danymi o ruchu – po wyrażeniu przez użytkowników uprzedniej zgody[5].

11 Jeżeli chodzi o informacje – w tym dane o lokalizacji – zbierane bezpośrednio z terminala, zastosowanie ma art. 5 ust. 3 dyrektywy. W związku z tym przechowywanie informacji na urządzeniu użytkownika lub uzyskanie dostępu do informacji już przechowywanych jest dozwolone wyłącznie wtedy, gdy (i) użytkownik wyraził na to zgodę[6] lub (ii) jeżeli przechowywanie tych informacji lub dostęp do nich są ściśle niezbędne w celu świadczenia usługi społeczeństwa informacyjnego wyraźnie zażądanej przez użytkownika.

12 Wyjątki od praw i obowiązków, o których mowa w dyrektywie, są jednak możliwe zgodnie z art. 15, jeżeli stanowią niezbędny, właściwy i proporcjonalny środek w ramach społeczeństwa demokratycznego do osiągnięcia pewnych celów[7].

13 Jeżeli chodzi o ponowne wykorzystywanie danych o lokalizacji gromadzonych przez podmiot świadczący usługi społeczeństwa informacyjnego do celów tworzenia modeli (np. za pośrednictwem systemu operacyjnego lub wcześniej zainstalowanej aplikacji), muszą zostać spełnione dodatkowe warunki. Jeżeli dane gromadzono zgodnie z art. 5 ust. 3 dyrektywy, można je przetwarzać dalej za dodatkową zgodą osoby, której dane dotyczą, lub na podstawie prawa Unii lub prawa państwa członkowskiego, które stanowią niezbędny i proporcjonalny środek w społeczeństwie demokratycznym do zabezpieczenia celów, o których mowa w art. 23 ust. 1 RODO[8].

2.2 Koncentracja na wykorzystywaniu zanonimizowanych danych o lokalizacji

14 EROD podkreśla, że jeżeli chodzi o wykorzystanie danych o lokalizacji, w pierwszej kolejności należy zawsze przetwarzać dane zanonimizowane, a nie dane osobowe.

15 Anonimizacja odnosi się do wykorzystania zestawu technik w celu uniemożliwienia powiązania danych ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną pomimo podjęcia wszelkich „rozsądnych" starań. „Test racjonalności" musi uwzględniać zarówno aspekty obiektywne (czas, środki techniczne), jak i elementy kontekstowe, które mogą się różnić w zależności od przypadku (rzadkość występowania danego zjawiska, przy wzięciu pod uwagę np. gęstości zaludnienia oraz charakteru i ilości danych). Jeżeli dane nie spełnią kryteriów tego testu, oznacza to, że nie zostały zanonimizowane, a zatem pozostają objęte zakresem RODO.

16 Ocena rzetelności anonimizacji zależy od trzech następujących kryteriów: (i) wyodrębnienia (wyizolowanie konkretnej osoby z większej grupy na podstawie danych); (ii) możliwości powiązania (powiązanie dwóch wpisów dotyczących tej samej osoby); oraz (iii) wnioskowania (wydedukowanie, z dużym prawdopodobieństwem, nieznanych informacji na temat konkretnej osoby).

17 Pojęcie anonimizacji jest często źle rozumiane i mylone z pojęciem pseudonimizacji. Podczas gdy anonimizacja umożliwia wykorzystanie danych bez żadnych ograniczeń, dane spseudonimizowane wciąż są objęte zakresem RODO.

18 Istnieje wiele możliwości skutecznej anonimizacji[9], jednak z pewnym zastrzeżeniem. Dane nie mogą zostać zanonimizowane same w sobie, tj. anonimizować można jedynie całe zbiory danych. W tym sensie każdą interwencję w pojedynczy wzorzec danych (z wykorzystaniem szyfrowania lub jakichkolwiek innych matematycznych przekształceń) można uznać w najlepszym wypadku za pseudonimizację.

19 Procesy anonimizacji i ataki mające na celu ponowną identyfikację to dziedziny, w których prowadzi się prężne badania. Kluczowe znaczenie dla każdego administratora wdrażającego rozwiązania z zakresu anonimizacji ma monitorowanie bieżących postępów w tej dziedzinie, zwłaszcza jeżeli chodzi o dane o lokalizacji (pochodzące od operatorów telekomunikacyjnych i/lub usług społeczeństwa informacyjnego), o których wiadomo, że niezwykle trudno jest je zanonimizować.

20 Rzeczywiście na podstawie licznych badań wykazano[10], że *dane o lokalizacji uważane za zanonimizowane* mogą w istocie nie być zanonimizowane. Ślady mobilności osób fizycznych są ze swej natury wysoce skorelowane i niepowtarzalne. W związku z tym mogą one w określonych okolicznościach być podatne na próby ponownej identyfikacji.

21 Nie można w pełni zanonimizować pojedynczego wzorca danych śledzącego przez dłuższy czas lokalizację danej osoby. Ocena ta może wciąż być prawdziwa, jeżeli dokładność zarejestrowanych współrzędnych geograficznych nie jest w istotny sposób obniżona lub jeżeli usunięto szczegółowe informacje na temat trasy oraz nawet jeśli zachowane jest wyłącznie położenie miejsc, w których przez znaczącą ilość czasu przebywa osoba, której dane dotyczą. Dotyczy to także słabo zagregowanych danych o lokalizacji.

22 Celem osiągnięcia anonimizacji dane o lokalizacji muszą być starannie przetwarzane w celu spełnienia wymogów testu racjonalności. W tym sensie takie przetwarzanie obejmuje rozpatrywanie zbiorów danych o lokalizacji jako całości oraz przetwarzanie danych pochodzących z racjonalnie dużego zbioru osób fizycznych z wykorzystaniem dostępnych rzetelnych technik anonimizacji, pod warunkiem że są one odpowiednio i skutecznie wdrożone.

23 Ponadto, biorąc pod uwagę złożoność procesów anonimizacji, usilnie zachęca się do zapewnienia przejrzystości w kwestii metodologii anonimizacji.

[4] Zob. art. 2 lit. c) dyrektywy.
[5] Zob. art. 6 i 9 dyrektywy.
[6] Pojęcie zgody w dyrektywie pozostaje pojęciem zgody w RODO i musi spełniać wszystkie wymogi dotyczące zgody określone w art. 4 pkt 11 oraz w art. 7 RODO.
[7] W celu interpretacji art. 15 dyrektywy należy odnieść się także do wyroku TSUE z dnia 29 stycznia 2008 r. w sprawie C-275/06, Productores de Música de España (Promusicae)/Telefónica de España SAU.
[8] Zob. sekcja 1.5.3 wytycznych 1/2020 w sprawie przetwarzania danych osobowych w kontekście pojazdów podłączonych do internetu.
[9] Y. De Montjoye i in. (2018) „On the privacy-conscientious use of mobile phone data".
[10] Y. De Montjoye i in. (2013) „Unique in the Crowd: The privacy bounds of human mobility" oraz A. Pyrgelis i in. (2017) „Knock Knock, Who's There? Membership Inference on Aggregate Location Data".

3 APLIKACJE SŁUŻĄCE DO USTALANIA KONTAKTÓW ZAKAŹNYCH

3.1 Ogólna analiza prawna

24 Systematyczne monitorowanie na dużą skalę lokalizacji osób fizycznych i/lub kontaktów między nimi stanowi poważną ingerencję w prywatność tych osób. Można je uzasadnić jedynie opierając się na dobrowolnym przyjęciu przez użytkowników każdego z odpowiednich celów. Oznaczałoby to w szczególności, że osoby, które nie zdecydują się na korzystanie z takich aplikacji lub nie mogą z takich aplikacji korzystać, nie powinny ponosić żadnych niekorzystnych konsekwencji.

25 Zapewnienie rozliczalności wymaga wyraźnego wskazania administratora każdej aplikacji służącej do ustalania kontaktów zakaźnych. EROD uważa, że administratorami[11] takich aplikacji mogłyby być krajowe organy ds. zdrowia; można uwzględnić także innych administratorów. We wszystkich przypadkach, jeżeli we wdrażanie aplikacji służących do ustalania kontaktów zakaźnych zaangażowane są różne podmioty, ich role i obowiązki muszą od samego początku być jasno określone i wyjaśnione użytkownikom.

26 Ponadto, jeżeli chodzi o zasadę ograniczenia celu, cele muszą być wystarczająco szczegółowe, by wykluczyć dalsze przetwarzanie danych do celów niezwiązanych z zarządzaniem kryzysem zdrowotnym COVID-19 (jak np. do celów komercyjnych lub egzekwowania prawa). Kiedy cel zostanie już jasno określony, konieczne będzie zapewnienie, aby wykorzystywanie danych osobowych było adekwatne, niezbędne i proporcjonalne.

27 W kontekście aplikacji służących do ustalania kontaktów zakaźnych należy starannie uwzględnić zasadę minimalizacji danych oraz uwzględniania ochrony danych w fazie projektowania i domyślnej ochrony danych:

- aplikacje służące do ustalania kontaktów zakaźnych nie wymagają śledzenia lokalizacji poszczególnych użytkowników. Zamiast tego należy korzystać z danych dotyczących bliskości fizycznej;
- ponieważ aplikacje służące do ustalania kontaktów zakaźnych mogą działać bez bezpośredniej identyfikacji poszczególnych osób, należy wdrożyć środki, które umożliwią zapobieganie ponownej identyfikacji;
- zgromadzone informacje powinny znajdować się na terminalu użytkownika i, gdy jest to bezwzględnie niezbędne, powinny być gromadzone tylko istotne informacje.

28 Jeżeli chodzi o zgodność przetwarzania z prawem, EROD zwraca uwagę, że stosowanie aplikacji służących do ustalania kontaktów zakaźnych obejmuje przechowywanie i/lub dostęp do informacji już przechowywanych na terminalu, co podlega pod art. 5 ust. 3 dyrektywy. Jeżeli operacje te są ściśle niezbędne, aby dostawca aplikacji mógł świadczyć usługę, której wyraźnie zażądał użytkownik, przetwarzanie nie wymaga zgody takiego użytkownika. Jeżeli chodzi o operacje, które nie są ściśle niezbędne, dostawca będzie musiał uzyskać zgodę użytkownika.

29 Ponadto EROD zwraca uwagę, że sam fakt, iż wykorzystanie aplikacji służących do ustalania kontaktów zakaźnych odbywa się na zasadzie dobrowolności, nie oznacza, że przetwarzanie danych osobowych będzie koniecznie odbywało się na podstawie zgody. Jeżeli organy publiczne świadczą usługę w oparciu o mandat przyznany przez prawo oraz zgodnie z określonymi w nim wymogami, najbardziej właściwą podstawą prawną przetwarzania jest niezbędność wykonania zadania realizowanego w interesie publicznym, tj. art. 6 ust. 1 lit. e) RODO.

30 W art. 6 ust. 3 RODO wyjaśniono, że podstawa przetwarzania, o którym mowa w art. 6 ust. 1 lit. e), musi być określona w prawie Unii lub w prawie państwa członkowskiego, któremu podlega administrator. Cel przetwarzania musi być określony w tej podstawie prawnej lub, w przypadku przetwarzania, o którym mowa w ust. 1 lit. e) – musi być ono niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi[12].

31 Podstawa prawna lub akt prawny, stanowiący zgodną z prawem podstawę stosowania aplikacji służących do ustalania kontaktów zakaźnych, powinny jednakże zawierać istotne zabezpieczenia, w tym odniesienie do dobrowolnego charakteru aplikacji. Należy w nich jasno określić cel oraz zawrzeć wyraźne ograniczenia dotyczące dalszego wykorzystywania danych osobowych, a także jednoznacznie wskazać zaangażowanego administratora lub administratorów. Należy określić także kategorie danych oraz podmioty, którym mogą zostać ujawnione dane osobowe (oraz cele, do których realizacji mogą zostać ujawnione takie dane). W zależności od poziomu ingerencji należy włączyć dodatkowe zabezpieczenia, z uwzględnieniem charakteru, zakresu i celów przetwarzania. Ponadto EROD zaleca także, aby w jak najkrótszym czasie uwzględnić kryteria pozwalające stwierdzić, kiedy aplikacja ma zostać usunięta, a także wskazać podmiot, który ponosi odpowiedzialność i będzie podlegać rozliczeniu za stwierdzenie tego.

32 Jeżeli jednak przetwarzanie danych opiera się na innej podstawie prawnej, takiej jak na przykład zgoda (art. 6 ust. 1 lit. a))[13], administrator będzie musiał zapewnić, aby spełnione zostały rygorystyczne wymagania dotyczące ważności takiej podstawy prawnej.

33 Ponadto wykorzystanie aplikacji do walki z pandemią COVID-19 może prowadzić do gromadzenia danych dotyczących zdrowia (na przykład statusu osoby zakażonej). Przetwarzanie takich danych jest dozwolone, kiedy jest ono niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, jeżeli zostaną spełnione warunki określone w art. 9 ust. 2 lit. i) RODO[14], lub do celów dotyczących opieki zdrowotnej, jak opisano w art. 9 ust. 2 lit. h) RODO[15]. W zależności od podstawy prawnej przetwarzanie może także odbywać się na podstawie wyraźnej zgody (art. 9 ust. 2 lit. a) RODO).

34 Zgodnie z pierwotnym celem w art. 9 ust. 2 lit. j) RODO dopuszcza się także możliwość przetwarzania danych dotyczących zdrowia, jeżeli jest to niezbędne do celów badań naukowych lub do celów statystycznych.

35 Trwający kryzys w dziedzinie zdrowia nie powinien być okazją do ustanawiania nieproporcjonalnych uprawnień do zatrzymywania danych. Ograniczenie przechowywania powinno uwzględniać rzeczywiste potrzeby oraz istotność danych z medycznego punktu widzenia (np. względy motywowane epidemiologicznie, takie jak okres inkubacji itd.), a dane osobowe powinny być przechowywane wyłącznie na czas trwania kryzysu wywołanego przez COVID-19. Następnie, co do zasady, wszystkie dane osobowe należy usunąć lub zanonimizować.

36 EROD uważa, że takie aplikacje mogą stanowić jedynie wsparcie dla tradycyjnych metod ustalania kontaktów zakaźnych przez wykwalifikowany personel służby zdrowia, który może stwierdzić, czy bliski kontakt może skutkować zakażeniem wirusem (np. kiedy ma miejsce kontakt z osobą chronioną przez odpowiedni sprzęt – kasjerem itp. – czy też nie), ale nie mogą ich zastąpić. EROD podkreśla, że procedury i procesy, takie jak odpowiednie algorytmy stosowane przez aplikacje służące do ustalania kontaktów zakaźnych, powinny działać pod ścisłym nadzorem wykwalifikowanego personelu, aby ograniczyć występowanie wyników fałszywie pozytywnych lub negatywnych. W szczególności zadanie polegające na udzielaniu porad dotyczących kolejnych kroków nie powinno opierać się jedynie na zautomatyzowanym przetwarzaniu.

[11] Zob. także: Komisja Europejska, „Wytyczne dotyczące aplikacji pomocnych w walce z pandemią COVID-19 w odniesieniu do ochrony danych", C(2020) 2523 final, Bruksela, 16.04.2020.

[12] Zob. motyw 41.

[13] Administratorzy (zwłaszcza organy publiczne) muszą zwracać szczególną uwagę na fakt, że zgody nie należy uważać za dobrowolną, jeżeli dana osoba nie ma rzeczywistego wyboru, aby odmówić zgody lub ją wycofać bez niekorzystnych konsekwencji.

[14] Przetwarzanie musi odbywać się na podstawie prawa Unii lub prawa państwa członkowskiego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową.

[15] Zob. art. 9 ust. 2 lit. h) RODO.

37 Aby zapewnić rzetelność, rozliczalność oraz, szeroko rzecz ujmując, zgodność z prawem, algorytmy muszą być możliwe do kontrolowania i powinny podlegać regularnym przeglądom niezależnych ekspertów. Kod źródłowy aplikacji powinien być publicznie udostępniony w celu jak najszerszego nad nim nadzoru.

38 W jakimś stopniu zawsze będą pojawiały się wyniki fałszywie pozytywne. Ponieważ identyfikacja ryzyka zakażenia może prawdopodobnie mieć duży wpływ na poszczególne osoby, na przykład pozostanie w samoizolacji aż do otrzymania negatywnego wyniku testu, niezbędna jest możliwość poprawiania danych i/lub późniejszych wyników analiz. To wszystko powinno oczywiście mieć zastosowanie wyłącznie do scenariuszy i wdrożeń w przypadkach, gdy dane są przetwarzane lub przechowywane w sposób technicznie umożliwiający wprowadzanie takich poprawek oraz gdy prawdopodobne jest wystąpienie niekorzystnych skutków, o których mowa powyżej.

39 Wreszcie EROD uważa, że przed wdrożeniem takiego narzędzia należy przeprowadzić ocenę skutków dla ochrony danych, ponieważ przetwarzanie jest w tym przypadku uważane za operację, która z dużym prawdopodobieństwem może powodować wysokie ryzyko (dane dotyczące zdrowia, przewidywane wdrożenie na szeroką skalę, systematyczne monitorowanie, wykorzystanie nowego rozwiązania technologicznego)[16]. EROD zdecydowanie zaleca publikowanie ocen skutków dla ochrony danych.

3.2 Zalecenia i wymagania funkcjonalne

40 Zgodnie z zasadą minimalizacji danych, oprócz innych środków ochrony danych w fazie projektowania oraz domyślnej ochrony danych[17], przetwarzane dane należy ograniczyć do ścisłego minimum. Aplikacja nie powinna gromadzić informacji niepowiązanych lub niepotrzebnych, takich jak np. stan cywilny, identyfikatory komunikacyjne, obiekty rejestru urządzeń, wiadomości, dzienniki połączeń, dane o lokalizacji, identyfikatory urządzeń itp.

41 Dane przesyłane za pośrednictwem aplikacji muszą obejmować jedynie pewne niepowtarzalne i spseudonimizowane identyfikatory, generowane przez aplikację i dla niej właściwe. Identyfikatory te muszą być regularnie odnawiane z częstotliwością stosowną do celu, jakim jest ograniczenie rozprzestrzeniania się wirusa oraz wystarczającą, aby ograniczyć ryzyko identyfikacji i fizycznego śledzenia poszczególnych osób.

42 Wdrożenia w celu ustalania kontaktów zakaźnych mogą być oparte na podejściu scentralizowanym lub zdecentralizowanym[18]. Oba rozwiązania należy uznawać za wykonalne, pod warunkiem że zastosowano odpowiednie środki bezpieczeństwa, a każde z nich ma pewne zalety i wady. Tym samym etap tworzenia koncepcji aplikacji powinien zawsze obejmować rzetelne rozważenie obu koncepcji i ostrożne wyważenie ich wpływu na ochronę danych osobowych/prywatności, a także ich ewentualnego wpływu na prawa osób fizycznych.

43 Każdy serwer podłączony do systemu ustalania kontaktów zakaźnych musi gromadzić wyłącznie historię kontaktów lub spseudonimizowane identyfikatory użytkownika, którego zdiagnozowano jako zakażonego w wyniku odpowiedniej oceny przeprowadzonej przez organy ds. zdrowia i dobrowolnego działania podjętego przez użytkownika. Ewentualnie serwer musi przechowywać wykaz spseudonimizowanych identyfikatorów zakażonych użytkowników lub ich historię kontaktów tylko przez okres potrzebny do poinformowania potencjalnie zakażonych użytkowników o ich narażeniu i nie powinien podejmować prób identyfikacji potencjalnie zakażonych użytkowników.

[16] Zob. Wytyczne Grupy Roboczej Art. 29 (przyjęte przez EROD) dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko" do celów rozporządzenia 2016/679.
[17] Zob. Wytyczne EROD 4/2019 w sprawie uwzględniania ochrony danych w fazie projektowania oraz domyślnej ochrony danych z art. 25.
[18] Ogólnie rzecz biorąc, rozwiązanie zdecentralizowane jest bardziej zgodne z zasadą minimalizacji danych.

44 Wdrażanie globalnej metody ustalania kontaktów zakaźnych obejmującej zarówno aplikacje, jak i ustalanie tradycyjnymi metodami, może w niektórych przypadkach wymagać przetwarzania dodatkowych informacji. W tym kontekście te dodatkowe informacje powinny pozostawać na terminalu użytkownika i być przetwarzane wyłącznie wtedy, gdy jest to bezwzględnie niezbędne, oraz za uprzednią konkretną zgodą użytkownika.

45 Należy stosować zgodne ze stanem obecnej wiedzy techniki kryptograficzne, aby zabezpieczyć dane przechowywane na serwerach oraz w aplikacjach, wymianę danych między aplikacjami oraz zdalny serwer. Musi odbywać się także wzajemne uwierzytelnianie między aplikacją a serwerem.

46 Zgłaszanie użytkowników przez aplikację jako osób zakażonych SARS-CoV-2 musi podlegać odpowiedniej autoryzacji, na przykład za pośrednictwem jednorazowego kodu przypisanego do spseudonimizowanej tożsamości osoby zakażonej i powiązanego ze stacją kontrolną lub pracownikiem służby zdrowia. Jeżeli nie można uzyskać potwierdzenia w bezpieczny sposób, nie powinno mieć miejsca przetwarzanie danych, które zakłada prawidłowość statusu użytkownika.

47 Administrator, we współpracy z organami publicznymi, musi jasno i wyraźnie poinformować o łączu, pod którym można pobrać oficjalną krajową aplikację służącą do ustalania kontaktów zakaźnych w celu ograniczenia ryzyka korzystania przez obywateli z aplikacji strony trzeciej.

4 PODSUMOWANIE

48 Świat stoi w obliczu poważnego kryzysu w dziedzinie zdrowia publicznego, wymagającego zdecydowanej reakcji, której skutki będą odczuwalne w zakresie wykraczającym poza bieżącą sytuację nadzwyczajną. Zautomatyzowane przetwarzanie danych i technologie cyfrowe mogą stanowić kluczowe elementy walki z COVID-19. Należy jednak uważać na „efekt zapadki". Naszym obowiązkiem jest zapewnienie, aby każdy środek wdrożony w tych nadzwyczajnych okolicznościach był niezbędny, ograniczony w czasie, miał minimalny wymiar i podlegał okresowym i rzeczywistym przeglądom, a także kontroli naukowej.

49 EROD podkreśla, że nie powinno dochodzić do sytuacji, w których trzeba wybierać między skuteczną reakcją na bieżący kryzys a ochroną naszych praw podstawowych: możemy osiągnąć oba te cele jednocześnie, a ponadto zasady ochrony danych mogą odegrać istotną rolę w walce z wirusem. Europejskie prawo ochrony danych osobowych pozwala na odpowiedzialne wykorzystywanie danych osobowych do celów związanych z zarządzaniem zdrowiem, zapewniając jednocześnie, aby w tym procesie nie doszło do osłabienia praw i wolności osób fizycznych.

W imieniu Europejskiej Rady Ochrony Danych

Przewodnicząca

(Andrea Jelinek)

ZAŁĄCZNIK – APLIKACJE SŁUŻĄCE DO USTALANIA KONTAKTÓW ZAKAŹNYCH
PRZEWODNIK ANALITYCZNY

0. Zastrzeżenie

Przedstawione poniżej wskazówki nie mają charakteru normatywnego ani nie są wyczerpujące, a niniejszy przewodnik ma na celu jedynie zapewnienie ogólnych wskazówek dla projektantów aplikacji służących do ustalania kontaktów zakaźnych i podmiotów, które je wdrażają. Można stosować także inne rozwiązania niż te, które opisano w niniejszym przewodniku, i mogą one być zgodne z prawem, o ile są zgodne z odpowiednimi ramami prawnymi (tj. z RODO oraz z dyrektywą).

Należy także zwrócić uwagę na fakt, że niniejszy przewodnik ma charakter ogólny. W związku z tym zaleceń i obowiązków opisanych w niniejszym dokumencie nie należy postrzegać jako wyczerpujących. Oceny należy przeprowadzać oddzielnie dla każdego przypadku, a poszczególne aplikacje mogą wymagać dodatkowych środków, których nie opisano w niniejszym przewodniku.

1. Streszczenie

W wielu państwach członkowskich zainteresowane strony rozważają wykorzystanie aplikacji służących do *ustalania kontaktów zakaźnych*, aby pomóc ludziom w rozpoznaniu, czy mieli kontakt z osobą zakażoną SARS-Cov-2.

Warunki, na których takie aplikacje mogą skutecznie przyczynić się do zarządzania pandemią, nie zostały jeszcze ustalone. Konieczne jest ustalenie ich przed rozpoczęciem wdrażania takich aplikacji. Istotne znaczenie ma jednak zapewnienie wytycznych, które dostarczą odpowiednich informacji zespołom projektantów zapoczątkowujących dany projekt, aby już od początku procesu projektowania można było zagwarantować ochronę danych osobowych.

Należy zwrócić uwagę na fakt, że niniejszy przewodnik ma charakter ogólny. W związku z tym zaleceń i obowiązków opisanych w niniejszym dokumencie nie należy postrzegać jako wyczerpujących. Oceny należy przeprowadzać oddzielnie dla każdego przypadku, a poszczególne aplikacje mogą wymagać dodatkowych środków, których nie opisano w niniejszym przewodniku. Niniejszy przewodnik ma na celu jedynie zapewnienie ogólnych wskazówek dla projektantów aplikacji służących do ustalania kontaktów zakaźnych i podmiotów, które je wdrażają.

Niektóre kryteria mogą wykraczać poza ścisłe wymogi wynikające z ram ochrony danych. Ich celem jest zapewnienie najwyższego poziomu przejrzystości celem uzyskania akceptacji społecznej dla aplikacji służących do ustalania kontaktów zakaźnych.

W tym celu wydawcy aplikacji służących do ustalania kontaktów zakaźnych powinni uwzględnić poniższe kryteria:

- korzystanie z takiej aplikacji musi być w pełni dobrowolne. Korzystanie z aplikacji nie może być warunkiem dostępu do jakichkolwiek praw gwarantowanych przepisami prawa. Osoby muszą nieprzerwanie mieć pełną kontrolę nad swoimi danymi i powinny mieć możliwość swobodnego decydowania, czy chcą korzystać z aplikacji;

- aplikacje służące do ustalania kontaktów zakaźnych z dużym prawdopodobieństwem mogą powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych oraz wymagać przeprowadzenia oceny skutków dla ochrony danych przed ich wdrożeniem;
- informacje o fizycznej bliskości między użytkownikami aplikacji można uzyskać bez konieczności lokalizowania użytkowników. Ten rodzaj aplikacji nie wymaga danych o lokalizacji, a zatem nie powinien wiązać się z ich wykorzystaniem;
- w przypadku zdiagnozowania u użytkownika zakażenia SARS-CoV-2 należy poinformować o tym jedynie osoby, z którymi użytkownik miał bliski kontakt w odpowiednim z epidemiologicznego punktu widzenia w celu ustalenia kontaktów zakaźnych okresie zatrzymywania danych;
- tego typu działanie aplikacji może wymagać, w zależności od wybranej architektury, zastosowania scentralizowanego serwera. W takim przypadku oraz zgodnie z zasadami minimalizacji danych i ochrony danych w fazie projektowania, dane przetwarzane przez scentralizowany serwer powinny być ograniczone do absolutnego minimum:
    - jeżeli użytkownik zostanie zdiagnozowany jako zakażony, informacje dotyczące osób, z którymi miał wcześniej bliski kontakt, lub identyfikatory przesyłane przez aplikację użytkownika mogą być zbierane tylko za jego zgodą. Należy ustalić metodę weryfikacji, która pozwoli na stwierdzenie, że dana osoba jest rzeczywiście zakażona, bez identyfikacji użytkownika. Z technicznego punktu widzenia można to osiągnąć poprzez ostrzeżenie osób z którymi doszło do kontaktu wyłącznie po interwencji pracownika służby zdrowia, np. za pomocą specjalnego jednorazowego kodu;
    - informacje przechowywane na serwerze centralnym nie powinny umożliwiać administratorowi danych identyfikacji użytkowników, co do których stwierdzono, że są zakażeni lub kontaktowali się z takimi użytkownikami, ani nie powinny umożliwiać wnioskowania wzorców kontaktów, które nie są potrzebne do wskazania odpowiednich kontaktów;
- działanie tego typu aplikacji wymaga transmisji danych, które są odczytywane przez urządzenia innych użytkowników i odsłuchania tych komunikatów:
    - wystarczająca jest wymiana spseudonimizowanych identyfikatorów pomiędzy urządzeniami mobilnymi użytkowników (jak np. komputery, tablety, zegarki połączone (ang. connected watches) itp.), np. poprzez ich transmisję (np. za pomocą technologii Bluetooth Low Energy);
    - identyfikatory muszą być generowane przy użyciu uwzględniających aktualny stan wiedzy procesów kryptograficznych;
    - identyfikatory muszą być regularnie odnawiane, aby zmniejszyć ryzyko ataków związanych z fizycznym śledzeniem i ataków opartych na identyfikacji osoby wskutek łączenia danych pochodzących z różnych źródeł;
- tego typu aplikacja musi posiadać zabezpieczenia, aby zagwarantować bezpieczne procesy techniczne. W szczególności:
    - aplikacja nie powinna przekazywać użytkownikom informacji pozwalających na wywnioskowanie tożsamości lub diagnozy innych osób. Serwer centralny nie może ani identyfikować użytkowników, ani wnioskować informacji o nich.

Zastrzeżenie: powyższe zasady odnoszą się do zakładanego celu aplikacji służących do *ustalania kontaktów zakaźnych* i tylko do tego celu, który polega na automatycznym informowaniu osób potencjalnie narażonych na kontakt z wirusem (bez konieczności ich identyfikacji). Operatorzy aplikacji i jej infrastruktury mogą być kontrolowani przez właściwy organ nadzorczy. Przestrzeganie całości lub części tych wytycznych nie jest w sposób konieczny wystarczające do zapewnienia pełnej zgodności z ramami prawnymi ochrony danych.

2. Definicje

Kontakt	W przypadku aplikacji służącej do ustalania kontaktów zakaźnych kontaktem jest użytkownik, który uczestniczył w interakcji z użytkownikiem potwierdzonym jako nosiciel wirusa, a czas trwania kontaktu i odległość stwarzają ryzyko znacznego narażenia na zakażenie wirusem. Parametry dotyczące czasu trwania narażenia i odległości między ludźmi muszą zostać oszacowane przez organy ds. zdrowia i mogą zostać określone w aplikacji.
Dane o lokalizacji	Termin ten odnosi się do wszystkich danych przetwarzanych w sieci łączności elektronicznej lub przez usługę łączności elektronicznej, wskazujących położenie geograficzne terminala użytkownika publicznie dostępnych usług łączności elektronicznej (zgodnie z definicją zawartą w dyrektywie), jak również do danych z potencjalnych innych źródeł, odnoszących się do: • szerokości, długości i wysokości urządzenia końcowego; • kierunku przekazu użytkownika lub • czasu, w którym informacja dla danej lokalizacji została zapisana.
Interakcja	W kontekście aplikacji służącej do ustalania kontaktów zakaźnych interakcję definiuje się jako wymianę informacji pomiędzy dwoma urządzeniami znajdującymi się w bliskiej odległości od siebie (w przestrzeni i czasie), w zakresie wykorzystywanej technologii łączności (np. Bluetooth). Definicja ta nie obejmuje lokalizacji dwóch użytkowników interakcji.
Nosiciel wirusa	W niniejszym dokumencie za nosicieli wirusa uznaje się użytkowników, którzy uzyskali pozytywny wynik testu na obecność wirusa i otrzymali oficjalną diagnozę od lekarzy lub ośrodków zdrowia.
Ustalanie kontaktów zakaźnych	Osoby, które miały bliski kontakt (według kryteriów, które zostaną określone przez epidemiologów) z osobą zakażoną wirusem, są w znacznym stopniu narażone na ryzyko zakażenia się i w konsekwencji na zakażenie innych osób. Ustalanie kontaktów zakaźnych to metodologia kontrolowania choroby, która rejestruje wszystkie osoby, które przebywały w bezpośredniej bliskości nosiciela wirusa, w celu sprawdzenia, czy są one narażone na ryzyko zakażenia i zastosowania wobec nich odpowiednich środków sanitarnych.

3. Informacje ogólne

OG-1	Aplikacja musi być narzędziem uzupełniającym tradycyjne techniki ustalania kontaktów zakaźnych (w szczególności wywiady z osobami zakażonymi), tj. stanowić część szerszego programu zdrowia publicznego. Musi być wykorzystywana tylko do momentu, gdy tradycyjne techniki ustalania kontaktów zakaźnych będą w stanie samodzielnie poradzić sobie z ilością nowych zakażeń.
OG-2	Najpóźniej w momencie podjęcia decyzji o „powrocie do normalności" przez właściwe organy publiczne należy wprowadzić procedurę mającą na celu zaprzestanie gromadzenia identyfikatorów (globalna dezaktywacja aplikacji, instrukcje dotyczące odinstalowania aplikacji, automatyczne odinstalowanie itp.) oraz uruchomienie procesu usuwania wszystkich zgromadzonych danych ze wszystkich baz danych (aplikacji mobilnych i serwerów).
OG-3	Kod źródłowy aplikacji i jej zaplecza musi być otwarty, a specyfikacje techniczne muszą być podane do wiadomości publicznej, tak aby każda zainteresowana strona mogła przeprowadzić audyt kodu, a w stosownych przypadkach – uczestniczyć w jego ulepszaniu, korygowaniu ewentualnych błędów i zapewnianiu przejrzystości przetwarzania danych osobowych.
OG-4	Etapy wdrażania aplikacji muszą umożliwiać stopniowe potwierdzanie jej skuteczności z punktu widzenia zdrowia publicznego. W tym celu należy wcześniej określić protokół oceny, określający wskaźniki pozwalające na zmierzenie skuteczności aplikacji.

4. Cele

CEL-1	Celem aplikacji musi być wyłącznie ustalanie kontaktów zakaźnych, aby osoby potencjalnie narażone na kontakt z SARS-CoV-2 mogły zostać ostrzeżone i otoczone opieką. Nie można wykorzystywać jej do innego celu.
CEL-2	Nie wolno stosować aplikacji do celów innych niż jej pierwotne zastosowanie, tj. monitorowanie przestrzegania kwarantanny lub środków izolacji i/lub dystansu społecznego.
CEL-3	Aplikacji nie wolno wykorzystywać do wyciągania wniosków dotyczących lokalizacji użytkowników na podstawie ich interakcji i/lub innych środków.

5. Kwestie funkcjonalne

FUNK-1	Aplikacja musi zapewniać funkcjonalność umożliwiającą informowanie użytkowników o tym, że mogli być potencjalnie narażeni na kontakt z wirusem, przy czym informacja ta opiera się na bliskości zarażonego użytkownika w okresie X dni przed pozytywnym wynikiem badania przesiewowego (wartość X jest określana przez organy ds. zdrowia).

FUNK-2	Aplikacja powinna zawierać zalecenia dla użytkowników zidentyfikowanych jako osoby potencjalnie narażone na kontakt z wirusem. Powinna ona przekazywać instrukcje dotyczące środków, których należy przestrzegać, oraz umożliwiać użytkownikowi zwrócenie się o poradę. W takich przypadkach obowiązkowa byłaby interwencja człowieka.
FUNK-3	Algorytm mierzący ryzyko zakażenia poprzez uwzględnienie czynników odległości i czasu, a tym samym określający, kiedy należy dodać kontakt do listy na potrzeby ustalania kontaktów zakaźnych, musi być w bezpieczny sposób konfigurowalny, aby uwzględnić najnowszą wiedzę na temat rozprzestrzeniania się wirusa.
FUNK-4	**Użytkownicy muszą zostać poinformowani w sytuacji, gdy byli narażeni na kontakt z wirusem**, lub muszą regularnie otrzymywać informacje o tym, czy byli narażeni na kontakt z wirusem w okresie inkubacji wirusa.
FUNK-5	Aplikacja powinna być interoperacyjna z innymi aplikacjami opracowanymi w państwach członkowskich, tak aby możliwe było skuteczne powiadamianie użytkowników podróżujących po różnych państwach członkowskich.

6. Dane

DANE-1	Aplikacja musi posiadać funkcję przesyłania i odbierania danych za pomocą technologii komunikacji bliskiego zasięgu, takich jak Bluetooth Low Energy, aby można było ustalić kontakty zakaźne.
DANE-2	Przesyłane dane muszą zawierać kryptograficznie silne pseudolosowe identyfikatory, generowane przez aplikację i właściwe dla danej aplikacji.
DANE-3	Ryzyko konfliktu między pseudolosowymi identyfikatorami powinno być wystarczająco niskie.
DANE-4	Identyfikatory pseudolosowe muszą być regularnie odnawiane, z częstotliwością wystarczającą do ograniczenia ryzyka ponownej identyfikacji, fizycznego śledzenia lub powiązania osób, przez kogokolwiek, w tym operatorów serwerów centralnych, innych użytkowników aplikacji lub nieuczciwe osoby trzecie. Identyfikatory te muszą być generowane przez aplikację użytkownika, ewentualnie w oparciu o materiał dostarczony przez serwer centralny.
DANE-5	Zgodnie z zasadą minimalizacji danych aplikacja nie może gromadzić danych innych niż te, które są ściśle niezbędne do celów ustalania kontaktów zakaźnych.
DANE-6	Aplikacja nie może gromadzić danych o lokalizacji do celów ustalania kontaktów zakaźnych. Dane o lokalizacji mogą być przetwarzane wyłącznie w celu umożliwienia aplikacji interakcji z podobnymi aplikacjami w innych państwach i powinny być precyzyjnie ograniczone do tego, co jest ściśle niezbędne do tego celu.

DANE-7	Aplikacja nie powinna gromadzić danych dotyczących zdrowia poza tymi, które są ściśle niezbędne do realizacji jej celów, z wyjątkiem dobrowolnego gromadzenia danych wyłącznie w celu pomocy w procesie podejmowania decyzji dotyczących informowania użytkownika.
DANE-8	Użytkownicy muszą być informowani o wszystkich danych osobowych, które będą gromadzone. Dane te powinny być zbierane tylko za zgodą użytkownika.

7. Właściwości techniczne

TECH-1	Aplikacja powinna wykorzystywać takie dostępne technologie, jak technologia komunikacji bliskiego zasięgu (np. Bluetooth Low Energy) w celu wykrywania użytkowników w pobliżu urządzenia z uruchomioną aplikacją.
TECH-2	Aplikacja powinna przechowywać historię kontaktów użytkownika na urządzeniu przez ograniczony, określony wcześniej czas.
TECH-3	Aplikacja może polegać na serwerze centralnym celem wdrożenia niektórych ze swoich funkcji.
TECH-4	Aplikacja musi bazować na architekturze, która w jak największym stopniu opiera się na urządzeniach użytkowników.
TECH-5	Użytkownicy zgłoszeni jako zakażeni wirusem, których status zostanie potwierdzony przez odpowiednio upoważnionego pracownika służby zdrowia, z własnej inicjatywy powinni przesłać historię swoich kontaktów lub własne identyfikatory na serwer centralny.

8. Bezpieczeństwo

BEZP-1	Mechanizm musi weryfikować status użytkowników, którzy w aplikacji oznaczyli się jako zakażeni SARS-CoV-2, np. poprzez podanie jednorazowego kodu powiązanego ze stacją badawczą lub pracownikiem służby zdrowia. Jeżeli nie można uzyskać potwierdzenia w bezpieczny sposób, dane nie mogą być przetwarzane.
BEZP-2	Dane wysyłane do serwera centralnego muszą być przesyłane bezpiecznym kanałem. Korzystanie z usług powiadamiania świadczonych przez dostawców platform systemu operacyjnego powinno podlegać dokładnej ocenie i nie powinno prowadzić do ujawnienia danych osobom trzecim.
BEZP-3	Żądania nie mogą być narażone na manipulowanie ze strony złośliwego użytkownika.
BEZP-4	Należy wdrożyć zgodne z aktualnym stanem wiedzy techniki kryptograficzne w celu zabezpieczenia wymiany informacji między aplikacją a serwerem oraz między aplikacjami, a także, co do zasady, w celu ochrony informacji przechowywanych w aplikacjach i na serwerze. Do przykładowych technik, które mogą być stosowane, zalicza się: szyfrowanie symetryczne i asymetryczne, funkcje skrótu, test prywatnego członkostwa (ang. *private membership test*), obliczanie części wspólnej zbiorów prywatnych (ang. *private set intersection*), filtry Blooma, odzyskiwanie informacji prywatnych, szyfrowanie homomorficzne itp.
BEZP-5	Serwer centralny nie może przechowywać identyfikatorów połączeń sieciowych (np. adresów IP) żadnych użytkowników, w tym tych, którzy zostali pozytywnie zdiagnozowani i przesłali historię swoich kontaktów lub własne identyfikatory.
BEZP-6	Aby uniknąć podszywania się lub tworzenia fałszywych użytkowników, serwer musi uwierzytelnić aplikację.
BEZP-7	Aplikacja musi uwierzytelnić serwer centralny.
BEZP-8	Funkcje serwera powinny być chronione przed atakami polegającymi na ponownym przesłaniu komunikatu przez złośliwą stronę trzecią (ang. *replay attacks*).
BEZP-9	Informacje przesyłane przez serwer centralny muszą zostać podpisane w celu uwierzytelnienia ich pochodzenia i integralności.
BEZP-10	Dostęp do wszystkich danych przechowywanych na serwerze centralnym, które nie są publicznie dostępne, musi być zastrzeżony wyłącznie dla osób upoważnionych.
BEZP-11	Na poziomie systemu operacyjnego menedżer uprawnień urządzenia może żądać jedynie uprawnień niezbędnych do uzyskania dostępu do modułów komunikacyjnych i korzystania z nich w razie potrzeby, do przechowywania danych w terminalu oraz do wymiany informacji z serwerem centralnym.

9. Ochrona danych osobowych i prywatności osób fizycznych

Przypomnienie: poniższe wytyczne dotyczą aplikacji, której jedynym celem jest ustalanie kontaktów zakaźnych.

PRYW-1	Wymiana danych musi odbywać się z poszanowaniem prywatności użytkowników (a w szczególności z poszanowaniem zasady minimalizacji danych).
PRYW-2	Aplikacja nie może umożliwiać bezpośredniej identyfikacji użytkowników podczas korzystania z niej.
PRYW-3	Aplikacja nie może pozwalać na śledzenie przemieszczania się użytkowników.
PRYW-4	Korzystanie z aplikacji nie powinno pozwalać użytkownikom na uzyskanie jakichkolwiek informacji o innych użytkownikach (a w szczególności o tym, czy są oni nosicielami wirusa czy nie).
PRYW-5	Zaufanie do serwera centralnego musi być ograniczone. Zarządzanie serwerem centralnym musi odbywać się zgodnie z jasno określonymi zasadami zarządzania i obejmować wszystkie środki niezbędne do zapewnienia jego bezpieczeństwa. Lokalizacja serwera centralnego powinna umożliwiać właściwemu organowi nadzorczemu prowadzenie skutecznego nadzoru.
PRYW-6	Należy przeprowadzić ocenę skutków dla ochrony danych i podać ją do wiadomości publicznej.
PRYW-7	Aplikacja powinna ujawniać użytkownikowi jedynie, czy był narażony na kontakt z wirusem, oraz - w miarę możliwości bez ujawniania informacji o innych użytkownikach - liczbę i daty takich zdarzeń.
PRYW-8	Z informacji przekazywanych przez aplikację użytkownicy nie powinni być w stanie zidentyfikować osób będących nosicielami wirusa ani śledzić ich ruchów.
PRYW-9	Z informacji przekazywanych przez aplikację organy ds. zdrowia nie powinny być w stanie zidentyfikować potencjalnie narażonych osób bez ich zgody.
PRYW-10	Żądania wysyłane przez aplikację do serwera centralnego nie mogą ujawniać żadnych informacji na temat nosiciela wirusa.
PRYW-11	Żądania wysyłane przez aplikację do serwera centralnego nie mogą ujawniać żadnych informacji o użytkowniku, które nie są niezbędne, za wyjątkiem gdy jest to możliwe i tylko wówczas, gdy jest to konieczne, jej spseudonimizowanych identyfikatorów i listy kontaktów.
PRYW-12	Nie może istnieć możliwość przeprowadzania ataków opartych na identyfikacji osób wskutek łączenia danych pochodzących z różnych źródeł (ang. linkage attacks).
PRYW-13	Użytkownicy muszą mieć możliwość wykonywania swoich praw za pośrednictwem aplikacji.
PRYW-14	Usunięcie aplikacji musi skutkować usunięciem wszystkich zebranych lokalnie danych.

PRYW-15	Aplikacja powinna gromadzić jedynie dane przekazywane przez instancje aplikacji lub interoperacyjne równoważne aplikacje. Nie powinny być zbierane żadne dane odnoszące się do innych aplikacji lub urządzeń łączności bliskiego zasięgu.
PRYW-16	Aby uniknąć ponownej identyfikacji przez serwer centralny, należy zastosować serwery proxy. Zadaniem tych *niezagrażających bezpieczeństwu serwerów* (ang.: non-colluding servers) jest mieszanie identyfikatorów kilku użytkowników (zarówno nosicieli wirusa, jak i osób wysyłających żądanie) przed udostępnieniem ich serwerowi centralnemu, tak aby ten nie poznał identyfikatorów (takich jak adresy IP) użytkowników.
PRYW-17	Należy starannie opracować i skonfigurować aplikację i serwer, aby nie gromadziły niepotrzebnych danych (np. w dziennikach serwera nie należy umieszczać żadnych identyfikatorów itp.) oraz aby uniknąć korzystania z SDK stron trzecich gromadzącego dane do innych celów.

W przypadku uznania użytkownika za zakażonego w większości omawianych obecnie aplikacji służących do ustalania kontaktów zakaźnych stosuje się zasadniczo dwa podejścia: mogą one albo wysłać na serwer historię kontaktów bezpośrednich, które uzyskały poprzez skanowanie, albo wysłać listę własnych identyfikatorów, które były transmitowane. Zgodnie z tymi dwoma podejściami odrzuca się następujące zasady. Chociaż podejścia te zostały omówione w niniejszych wytycznych, nie oznacza to, że inne podejścia nie są możliwe lub nawet preferowane, np. podejścia, w ramach których wykorzystuje się pewną formę szyfrowania E2E lub stosuje inne technologie służące wzmocnieniu ochrony bezpieczeństwa i prywatności.

9.1. Zasady, które obowiązują tylko wtedy, **gdy aplikacja przesyła listę kontaktów na serwer**

KON-1	Serwer centralny musi zebrać historię kontaktów użytkowników zgłoszonych jako osoby zakażone SARS-CoV-2, w wyniku dobrowolnego działania z ich strony.
KON-2	Serwer centralny nie może przechowywać ani rozpowszechniać listy spseudonimizowanych identyfikatorów użytkowników będących nosicielami wirusa.
KON-3	Historia kontaktów przechowywana na serwerze centralnym musi zostać usunięta po powiadomieniu użytkowników o ich bliskim kontakcie z osobą zakażoną.
KON-4	Z wyjątkiem przypadków, gdy użytkownik, w przypadku którego ustalono, iż ma pozytywny wynik testu, udostępnia swoją historię kontaktów na serwerze centralnym lub gdy wysyła na serwer prośbę o przekazanie informacji o potencjalnym narażeniu na wirusa, żadne dane nie mogą opuścić urządzenia użytkownika.
KON-5	Każdy identyfikator zawarty w lokalnej historii musi zostać usunięty po upływie X dni od jego dodania (wartość X jest określana przez organy ds. zdrowia).
KON-6	Historie kontaktów przekazywane przez różnych użytkowników nie powinny być dalej przetwarzane, np. wzajemnie korelowane w celu stworzenia globalnych map bezpośrednich kontaktów.

KON-7	Dane w dziennikach serwera muszą być ograniczone do minimum i muszą być zgodne z wymogami ochrony danych.

9.2. Zasady, które obowiązują tylko wtedy, gdy aplikacja przesyła listę własnych identyfikatorów na serwer

ID-1	Serwer centralny musi zebrać identyfikatory przesłane przez aplikację użytkowników zgłoszonych jako osoby zakażone SARS-CoV-2, w wyniku dobrowolnego działania z ich strony.
ID-2	Serwer centralny nie może przechowywać ani rozpowszechniać historii kontaktów użytkowników będących nosicielami wirusa.
ID-3	Identyfikatory przechowywane na serwerze centralnym muszą zostać usunięte po ich rozesłaniu do pozostałych aplikacji.
ID-4	Z wyjątkiem przypadków, gdy użytkownik, w przypadku którego ustalono, iż ma pozytywny wynik testu, udostępnia swoje identyfikatory na serwerze centralnym lub gdy wysyła na serwer prośbę o przekazanie informacji o potencjalnym narażeniu na wirusa, żadne dane nie mogą opuścić urządzenia użytkownika.
ID-5	Dane w dziennikach serwera muszą być zminimalizowane i muszą być zgodne z wymogami ochrony danych.



Wytyczne 03/2020 w sprawie przetwarzania danych dotyczących zdrowia do celów badań naukowych w kontekście pandemii COVID-19

Przyjęte 21 kwietnia 2020 r.

Historia wersji

Wersja 1.1	30 kwietnia 2020 r.	Drobne korekty
Wersja 1.0	21 kwietnia 2020 r.	Przyjęcie wytycznych

Spis treści

1 Wprowadzenie 4
2 Zastosowanie RODO 4
3 Definicje 5
3.1 „Dane dotyczące zdrowia” 5
3.2 „Przetwarzanie do celów badań naukowych” 5
3.3 „Dalsze przetwarzanie” 6
4 Podstawa prawna przetwarzania 6
4.1 Zgoda 6
4.2 Przepisy krajowe 7
5 Zasady ochrony danych 8
5.1 Przejrzystość i obowiązek informacyjny względem osób, których dane dotyczą 8
5.1.1 Kiedy należy poinformować osobę, której dane dotyczą? 8
5.1.2 Odstępstwa 9
5.2 Ograniczenie celu i domniemanie zgodności 10
5.3 Minimalizacja danych i ograniczenie przechowywania danych 10
5.4 Integralność i poufność 11
6 Wykonywanie przez osoby, których dane dotyczą, przysługujących im praw 12
7 Międzynarodowe przekazywanie danych do celów badań naukowych 12
8 Podsumowanie 14

Europejska Rada Ochrony Danych

uwzględniając art. 70 ust. 1 lit. e) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (zwanego dalej „RODO"),

uwzględniając Porozumienie EOG, w szczególności załącznik XI i protokół 37 do tego Porozumienia, zmienione decyzją Wspólnego Komitetu EOG nr 154/2018 z dnia 6 lipca 2018 r.,

uwzględniając art. 12 i 22 swojego regulaminu wewnętrznego,

PRZYJĘŁA NASTĘPUJĄCE WYTYCZNE:

1 WPROWADZENIE

1. W obliczu pandemii COVID-19 podejmuje się obecnie ogromne starania w ramach badań naukowych w celu walki z SARS-CoV-2, aby jak najszybciej osiągnąć wyniki badań.

2. Jednocześnie wciąż pojawiają się kwestie prawne w związku z wykorzystaniem danych dotyczących zdrowia zgodnie z art. 4 pkt 15 RODO do celów takich badań naukowych. Niniejsze wytyczne mają na celu omówienie najpilniejszych z tych kwestii, takich jak podstawa prawna, wdrożenie odpowiednich zabezpieczeń do celów tego rodzaju przetwarzania danych dotyczących zdrowia, a także wykonywanie praw osób, których dane dotyczą.

3. Należy zwrócić uwagę, że opracowanie dalszych, bardziej szczegółowych wytycznych w sprawie przetwarzania danych dotyczących zdrowia do celów badań naukowych stanowi część rocznego planu prac EROD. Ponadto w obecnych wytycznych nie koncentrowano się na kwestii przetwarzania danych osobowych do celów nadzoru epidemiologicznego.

2 ZASTOSOWANIE RODO

4. Przepisy o ochronie danych (takie jak RODO) nie utrudniają realizacji działań podejmowanych w walce z pandemią COVID-19[1]. RODO jest aktem prawnym o szerokim zakresie i zawiera szereg przepisów umożliwiających przetwarzanie danych osobowych do celów badań naukowych związanych z pandemią COVID-19 zgodnie z prawami podstawowymi do prywatności i ochrony danych osobowych[2]. W RODO przewidziano również specjalny wyjątek od zakazu przetwarzania niektórych szczególnych kategorii danych osobowych, takich jak dane dotyczące zdrowia, jeżeli jest to niezbędne do tych celów badań naukowych. [3]

5. Przy przetwarzaniu danych dotyczących zdrowia do celów badań naukowych związanych z pandemią COVID-19 należy zapewnić poszanowanie praw podstawowych UE. Ani przepisy o ochronie danych, ani wolność nauki przewidziana w art. 13 Karty praw podstawowych Unii Europejskiej nie mają nad sobą pierwszeństwa. Zamiast tego należy starannie ocenić i wyważyć te prawa i wolności, aby osiągnąć rezultat, który będzie zgodny z duchem obu tych zasad.

[1] Zob. oświadczenie EROD w sprawie ogólnego przetwarzania danych osobowych w kontekście pandemii COVID-19 z dnia 19 marca 2020 r. dostępne pod adresem https://edpb.europa.eu/our-work-tools/our-documents/other/statement-processing-personal-data-context-covid-19-outbreak_en.

[2] Zob. na przykład art. 5 ust. 1 lit. b) i e), art. 14 ust. 5 lit. b) oraz art. 17 ust. 3 lit. d) RODO.

[3] Zob. na przykład art. 9 ust. 2 lit. j) oraz art. 89 ust. 2 RODO.

3 DEFINICJE

6. Ważne jest, aby zrozumieć, które operacje przetwarzania podlegają specjalnemu systemowi przewidzianemu w RODO i przedstawionemu bardziej szczegółowo w niniejszych wytycznych. Dlatego też należy zdefiniować pojęcia: „dane dotyczące zdrowia", „przetwarzanie do celów badań naukowych" oraz „dalsze przetwarzanie" (zwane również „pierwotnym i wtórnym wykorzystaniem danych dotyczących zdrowia").

3.1 „Dane dotyczące zdrowia"

7. Zgodnie z art. 4 pkt 15 RODO „dane dotyczące zdrowia" oznaczają „dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej, w tym o korzystaniu z usług opieki zdrowotnej, ujawniające informacje o stanie jej zdrowia" Jak wskazano w motywie 53, dane dotyczące zdrowia zasługują na większą ochronę, ponieważ wykorzystanie takich danych wrażliwych może mieć istotne negatywne skutki dla osób, których te dane dotyczą. Z uwagi na ten fakt i w świetle stosownego orzecznictwa Europejskiego Trybunału Sprawiedliwości Unii Europejskiej (TSUE)[4] należy zastosować szeroką interpretację definicji „danych dotyczących zdrowia".

8. Dane dotyczące zdrowia mogą pochodzić z różnych źródeł – mogą to być na przykład:

   1. informacje zebrane przez świadczeniodawcę opieki zdrowotnej w dokumentacji medycznej pacjenta (w postaci wywiadu chorobowego lub wyników badań bądź terapii);
   2. informacje, które stały się danymi dotyczącymi zdrowia w wyniku ich odniesienia do innych danych, co ujawniło stan zdrowia lub zagrożenia dla zdrowia (takie jak założenie, że u danej osoby występuje większe ryzyko zawału serca ze względu na wysokie ciśnienie krwi, jakie odnotowano w ramach pomiarów prowadzonych przez określony czas);
   3. informacje przekazane w ankietach „samokontroli" przez osoby, których dane dotyczą, w ramach udzielanych odpowiedzi na pytania dotyczące ich stanu zdrowia (na przykład opisy objawów);
   4. informacje, które stały się danymi dotyczącymi zdrowia ze względu na ich wykorzystanie w określonym kontekście (np. informacje dotyczące niedawnej podróży lub obecności w regionie dotkniętym COVID-19, przetwarzane przez pracownika służby zdrowia w celu postawienia diagnozy).

3.2 „Przetwarzanie do celów badań naukowych"

9. W art. 4 RODO nie zawarto wyraźnej definicji „przetwarzania do celów badań naukowych". Jak wskazano w motywie 159, „przetwarzanie danych osobowych do celów badań naukowych należy interpretować szeroko, obejmując tym pojęciem na przykład rozwój technologiczny i demonstrację, badania podstawowe, badania stosowane oraz badania finansowane ze środków prywatnych. Ponadto należy uwzględnić cel Unii określony w art. 179 ust. 1 TFUE, którym jest utworzenie europejskiej przestrzeni badawczej. Wyrażenie »do celów badań naukowych« powinno obejmować także badania prowadzone w interesie publicznym w dziedzinie zdrowia publicznego".

[4] Zob. na przykład w odniesieniu do dyrektywy 95/46/WE wyrok Trybunału Sprawiedliwości Unii Europejskiej z dnia 6 listopada 2003 r., sprawa C-101/01 (Lindqvist), pkt 50.

10. Była Grupa Robocza Art. 29 wskazała już, że pojęcia tego nie można jednak rozszerzać poza jego powszechne znaczenie, i jest zdania, że w tym kontekście „badania naukowe" oznaczają „projekt badawczy zorganizowany zgodnie z normami metodycznymi i etycznymi w danym sektorze oraz zgodnie z dobrymi praktykami"[5].

3.3 „Dalsze przetwarzanie"

11. W kontekście „przetwarzania danych dotyczących zdrowia do celów badań naukowych" istnieją dwa rodzaje wykorzystania danych:

    1. badania dotyczące danych osobowych (dotyczących zdrowia), polegające na wykorzystaniu danych zebranych bezpośrednio do celów badań naukowych („wykorzystanie pierwotne");
    2. badania dotyczące danych osobowych (dotyczących zdrowia) polegające na dalszym przetwarzaniu danych zebranych początkowo do innego celu („wykorzystanie wtórne").

12. **Przykład 1:** Do celów przeprowadzenia badania klinicznego u osób, w przypadku których istnieje podejrzenie, że są one zakażone SARS-CoV-2, zbierane są dane dotyczące zdrowia i wykorzystywane są kwestionariusze. Zgodnie z powyższą definicją jest to „wykorzystanie pierwotne" danych dotyczących zdrowia.

13. **Przykład 2:** Osoba, której dane dotyczą, zgłosiła się do świadczeniodawcy opieki zdrowotnej jako pacjent z objawami typowymi dla SARS-CoV-2. Jeśli dane dotyczące zdrowia zebrane przez świadczeniodawcę opieki zdrowotnej zostaną później wykorzystane do celów badań naukowych, takie wykorzystanie klasyfikuje się jako dalsze przetwarzanie danych dotyczących zdrowia zebranych w innym celu (wykorzystanie wtórne).

14. Rozróżnienie między badaniami naukowymi opartymi na podstawowym wykorzystaniu danych dotyczących zdrowia a badaniami opartymi na wtórnym wykorzystaniu takich danych będzie miało szczególne znaczenie w dyskusjach dotyczących podstawy prawnej przetwarzania, obowiązków informacyjnych oraz zasady ograniczenia celu na mocy art. 5 ust. 1 lit. b) RODO, jak przedstawiono poniżej.

4 PODSTAWA PRAWNA PRZETWARZANIA

15. Dane osobowe dotyczące zdrowia muszą być w każdym przypadku przetwarzane zgodnie z zasadami związanymi z przetwarzaniem określonymi w art. 5 RODO oraz zgodnie z co najmniej jedną podstawą prawną i jednym szczególnym wyjątkiem wymienionymi odpowiednio w art. 6 i 9 RODO w celu zgodnego z prawem przetwarzania tej szczególnej kategorii danych osobowych[6].

16. Podstawy prawne i mające zastosowanie wyjątki odnośnie do przetwarzania danych dotyczących zdrowia do celów badań naukowych zawarto odpowiednio w art. 6 i 9. W następnej sekcji omówiono zasady dotyczące zgody i odpowiednie przepisy krajowe. Należy zauważyć, że nie istnieje hierarchia podstaw prawnych przewidzianych w RODO.

4.1 Zgoda

17. Zgoda osoby, której dane dotyczą, zebrana zgodnie z art. 6 ust. 1 lit. a) i art. 9 ust. 2 lit. a) RODO może stanowić podstawę prawną przetwarzania danych dotyczących zdrowia w kontekście COVID-19.

18. Należy jednak zauważyć, że konieczne jest spełnienie wszystkich warunków wyraźnej zgody, w szczególności tych określonych w art. 4 pkt 11, art. 6 ust. 1 lit. a), art. 7 oraz art. 9 ust. 2 lit. a) RODO. W szczególności zgoda musi być dobrowolna, konkretna, świadoma i jednoznaczna, a także wyrażona w formie oświadczenia lub „wyraźnego działania potwierdzającego".

19. Jak stwierdzono w motywie 43, zgody nie można uznać za udzieloną dobrowolnie, jeśli istnieje wyraźny brak równowagi między osobą, której dane dotyczą, a administratorem. Dlatego ważne jest, aby osoba, której dane dotyczą, nie była poddawana naciskom i nie ponosiła negatywnych konsekwencji w przypadku niewyrażenia zgody. EROD odniosła się już do kwestii zgody w kontekście badań klinicznych[7]. Dalsze wskazówki, w szczególności na temat wyraźnej zgody, można znaleźć w wytycznych dotyczących zgody wydanych przez byłą Grupę Roboczą Art. 29[8].

20. **Przykład:** W ramach nieinterwencyjnego badania danej populacji przeprowadzana jest ankieta badająca objawy i postęp choroby. Na potrzeby przetwarzania takich danych dotyczących zdrowia naukowcy mogą zwrócić się do osoby, której dane dotyczą, o zgodę na warunkach określonych w art. 7 RODO.

21. W opinii EROD powyższego przykładu *nie* uważa się za przypadek „wyraźnego braku równowagi sił", o którym mowa w motywie 43, a osoba, której dane dotyczą, powinna mieć możliwość udzielenia zgody badaczom[9]. W tym przykładzie między osobami, których dane dotyczą, a badaczami nie występuje jakakolwiek zależność, która mogłaby w niewłaściwy sposób wpłynąć na korzystanie przez te osoby z ich wolnej woli, a także jest oczywiste, że odmowa wyrażenia zgody nie będzie miała dla tych osób żadnych negatywnych konsekwencji.

22. Naukowcy powinni mieć jednak świadomość, że jeśli zgoda ma zostać wykorzystana jako podstawa prawna przetwarzania, musi istnieć możliwość wycofania tej zgody przez osoby fizyczne w dowolnym momencie na mocy art. 7 ust. 3 RODO. W przypadku wycofania zgody wszystkie operacje przetwarzania danych, które były oparte na zgodzie, pozostają zgodne z prawem na mocy RODO. Administrator musi jednak zaprzestać dalszych działań przetwarzania, a jeśli nie dysponuje inną podstawą prawną uzasadniającą zatrzymanie danych w celu dalszego przetwarzania, powinien je usunąć[10].

4.2 Przepisy krajowe

23. Art. 6 ust. 1 lit. e) lub art. 6 ust. 1 lit. f) RODO w związku z wyjątkami wprowadzonymi na mocy art. 9 ust. 2 lit. j) lub art. 9 ust. 2 lit. i) RODO może stanowić podstawę prawną do przetwarzania danych osobowych (dotyczących zdrowia) do celów badań naukowych. Rada udzieliła już stosownych wyjaśnień w kontekście badań klinicznych[11].

[5] Zob. wytyczne dotyczące zgody na mocy rozporządzenia 2016/679 byłej Grupy Roboczej Art. 29 z dnia 10 kwietnia 2018 r., WP259 rev.01, 17EN, s. 27 (w wersji EN) (zatwierdzone przez EROD). Dostępne pod adresem https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051 (przedmiotowy fragment znajduje się na st. 31 polskiej wersji językowej wytycznych dostępnej pod powyższym adresem)

[6] Zob. na przykład w odniesieniu do dyrektywy 95/46/WE wyrok Trybunału Sprawiedliwości Unii Europejskiej z dnia 13 maja 2014 r., sprawa C-131/12 (Google Hiszpania), pkt 71.

[7] Zob. opinia 3/2019 EROD z dnia 23 stycznia 2019 r. w sprawie pytań i odpowiedzi dotyczących wzajemnych zależności między rozporządzeniem w sprawie badań klinicznych (RBK) a ogólnym rozporządzeniem o ochronie danych (RODO), dostępna pod adresem: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinionctrq_a_final_pl.pdf.

[8] Wytyczne dotyczące zgody na mocy rozporządzenia 2016/679 byłej Grupy Roboczej Art. 29 z dnia 10 kwietnia 2018 r., WP259 rev.01, 17PL, s. 18 (zatwierdzone przez EROD).

[9] Przy założeniu, że osoba, której dane dotyczą, nie była poddawana naciskom ani nie grożono jej negatywnymi konsekwencjami, gdyby nie udzieliła zgody.

[10] Zob. art. 17 ust. 1 lit. b) i art. 17 ust. 3 RODO.

[11] Zob. opinia 3/2019 EROD z dnia 23 stycznia 2019 r., s. 7.

24. **Przykład:** Duże badanie populacji przeprowadzone w oparciu o karty chorób pacjentów z COVID-19.

25. Jak wskazano powyżej, zarówno UE, jak i prawodawca krajowy każdego państwa członkowskiego mogą przyjąć szczególne przepisy zgodnie z art. 9 ust. 2 lit. j) lub art. 9 ust. 2 lit. i) RODO, aby zapewnić podstawę prawną przetwarzania danych osobowych (dotyczących zdrowia) do celów badań naukowych. W związku z tym warunki i zakres takiego przetwarzania *różnią się* w zależności od przepisów przyjętych w danym państwie członkowskim.

26. Jak wskazano w art. 9 ust. 2 lit. i) RODO, w przepisach takich należy przewidzieć „odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową". Jak podobnie wskazano w art. 9 ust. 2 lit. j) RODO, takie przyjęte przepisy „są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą".

27. Ponadto przyjęte przepisy należy interpretować w świetle zasad określonych na mocy art. 5 RODO i z uwzględnieniem orzecznictwa Trybunału Sprawiedliwości Unii Europejskiej. W szczególności wyjątki i ograniczenia w związku z ochroną danych przewidziane w art. 9 ust. 2 lit. j) i art. 89 RODO muszą być stosowane tylko w takim zakresie, w jakim jest to absolutnie konieczne[12].

5 ZASADY OCHRONY DANYCH

28. Zarówno administrator, jak i podmiot przetwarzający dane osobowe muszą przestrzegać zasad dotyczących przetwarzania danych osobowych zgodnie z art. 5 RODO, w szczególności biorąc pod uwagę potencjalne przetwarzanie dużej ilości danych osobowych do celów badań naukowych. Najważniejsze aspekty tych zasad zostały omówione poniżej w kontekście niniejszych wytycznych.

5.1 Przejrzystość i obowiązek informacyjny względem osób, których dane dotyczą

29. Zasada przejrzystości oznacza, że dane osobowe są przetwarzane rzetelnie i w sposób przejrzysty w stosunku do osoby, której dane dotyczą. Zasada ta jest silnie związana z obowiązkami informacyjnymi wynikającymi z art. 13 lub art. 14 RODO.

30. Ogólnie osoba, której dane dotyczą, musi zostać indywidualnie poinformowana o prowadzeniu operacji przetwarzania oraz o tym, że dane osobowe (dotyczące zdrowia) są przetwarzane do celów naukowych. Dostarczone informacje powinny zawierać wszystkie elementy określone w art. 13 lub art. 14 RODO.

31. Należy zauważyć, że naukowcy często przetwarzają dane dotyczące zdrowia, których nie pozyskali bezpośrednio od osoby, której dane dotyczą, na przykład wykorzystując dane z dokumentacji medycznej pacjentów lub dane od pacjentów z innych krajów. Dlatego też w tej sekcji skoncentrowano się na art. 14 RODO, który dotyczy obowiązków informacyjnych w przypadkach, gdy dane osobowe nie są zbierane bezpośrednio od osoby, której dane dotyczą.

5.1.1 Kiedy należy poinformować osobę, której dane dotyczą?

32. Jeżeli dane osobowe nie zostały pozyskane od osoby, której dane dotyczą, art. 14 ust. 3 lit. a) RODO stanowi, że administrator musi jej podać informacje „w rozsądnym terminie po pozyskaniu danych osobowych – najpóźniej w ciągu miesiąca – mając na uwadze konkretne okoliczności przetwarzania danych osobowych".

[12] Zob. na przykład w odniesieniu do dyrektywy 95/46/WE wyrok Trybunału Sprawiedliwości z dnia 14 lutego 2019 r., sprawa C-345/17 (Buivids), pkt 64.

33. W obecnym kontekście należy w szczególności zwrócić uwagę na art. 14 ust. 4 RODO, który stanowi, że „jeżeli administrator planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym te dane zostały pozyskane, przed takim dalszym przetwarzaniem informuje on osobę, której dane dotyczą, o tym innym celu".

34. W przypadku dalszego przetwarzania danych do celów naukowych oraz biorąc pod uwagę wrażliwość przetwarzanych danych, odpowiednim zabezpieczeniem zgodnie z art. 89 ust. 1 jest podanie informacji osobie, której dane dotyczą, w rozsądnym terminie *przed* rozpoczęciem nowego projektu badawczego. Pozwala to osobie, której dane dotyczą, na zapoznanie się z projektem badawczym i daje jej możliwość wcześniejszego wykonania przysługujących jej praw.

5.1.2 Odstępstwa

35. W art. 14 ust. 5 RODO przewidziano jednak cztery odstępstwa od obowiązku informacyjnego. W obecnym kontekście szczególne znaczenie mają art. 14 ust. 5 lit. b) („okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku") i lit. c) („pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem Unii lub prawem państwa członkowskiego") RODO, zwłaszcza w odniesieniu do obowiązku informacyjnego na podstawie art. 14 ust. 4 RODO.

5.1.2.1 Okazuje się niemożliwe

36. Była Grupa Robocza Art. 29 zauważyła już w swoich wytycznych w sprawie przejrzystości[13], że „sytuacja, w której zgodnie z art. 14 ust. 5 lit. b) udzielenie informacji »okazuje się niemożliwe«, jest sytuacją zero-jedynkową, ponieważ dana sytuacja albo jest niemożliwa, albo jest możliwa; nie istnieją stopnie »niemożliwości«. Jeżeli administrator danych zamierza powołać się na to odstępstwo, musi wskazać czynniki, które faktycznie uniemożliwiają mu udzielenie odnośnych informacji osobom, których dane dotyczą. Jeżeli po upływie określonego czasu czynniki, które spowodowały »niemożliwość«, przestaną istnieć i administrator danych uzyska możliwość udzielenia informacji osobom, których dane dotyczą, powinien bezzwłocznie to uczynić. W praktyce istnieje bardzo niewiele sytuacji, w których administrator danych może wykazać faktyczną niemożliwość udzielenia informacji osobom, których dane dotyczą".

5.1.2.2 Niewspółmiernie duży wysiłek

37. W ramach ustalania, co stanowi niewspółmiernie duży wysiłek, w motywie 62 jako możliwe czynniki wskazano liczbę osób, których dane dotyczą, okres przechowywania oraz przyjęte odpowiednie zabezpieczenia. We wspomnianych powyżej wytycznych w sprawie przejrzystości[14] zaleca się, aby administrator danych przeprowadził test równowagi, aby porównać wysiłek wkładany przez administratora danych w udzielenie informacji osobom, których dane dotyczą, z konsekwencjami i skutkami dla tych osób w przypadku nieudzielenia tego rodzaju informacji.

38. **Przykład:** Za niewspółmiernie duży wysiłek do celów dostarczenia tych informacji można by uznać sytuację, w której istnieje duża liczba osób, których dane dotyczą, i brak jest dostępnych informacji kontaktowych.

[13] Zob. wytyczne w sprawie przejrzystości na podstawie rozporządzenia 2016/679 byłej Grupy Roboczej Art. 29 z dnia 11 kwietnia 2018 r., WP260 rev.01, 17/EN, s. 29 (zatwierdzone przez EROD). Dostępne pod adresem https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227.

[14] Wytyczne w sprawie przejrzystości na podstawie rozporządzenia 2016/679 byłej Grupy Roboczej Art. 29 z dnia 11 kwietnia 2018 r., WP260 rev.01, 17/EN, s. 31 (zatwierdzone przez EROD).

5.1.2.3 Poważne utrudnienie realizacji celów

39. Aby powołać się na to odstępstwo, administratorzy danych muszą wykazać, że udzielenie informacji określonych w art. 14 ust. 1 jako takie uniemożliwi lub poważnie utrudni realizację celów przetwarzania.

40. W przypadku, gdy ma zastosowanie odstępstwo przewidziane w art. 14 ust. 5 lit. b) RODO, „administrator podejmuje odpowiednie środki, by chronić prawa i wolności oraz prawnie uzasadnione interesy osoby, której dane dotyczą, w tym udostępnia informacje publicznie".

5.1.2.4 Pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem Unii lub państwa członkowskiego

41. W art. 14 ust. 5 lit. c) RODO dopuszcza się wyjątek od wymogów udzielenia informacji określonych w art. 14 ust. 1 ust. 2 i ust. 4, o ile pozyskiwanie lub ujawnianie danych osobowych „jest wyraźnie uregulowane prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator". Odstępstwo to jest zależne od przedmiotowego prawa przewidującego „odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą". Jak stwierdzono we wspomnianych wyżej wytycznych w sprawie przejrzystości[15], prawo takie musi bezpośrednio odnosić się do administratora danych, a przedmiotowe pozyskiwanie lub ujawnianie powinno być obowiązkowe dla administratora danych. EROD przypomina, że w przypadku korzystania z tego odstępstwa administrator danych musi być w stanie wykazać, w jaki sposób dane prawo ma do niego zastosowanie. Odstępstwo to wymaga również od administratora danych uzyskania albo ujawnienia danych osobowych, o których mowa.

5.2 Ograniczenie celu i domniemanie zgodności

42. Na mocy art. 5 ust. 1 lit. b) RODO dane powinny być co do zasady „zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami".

43. W ramach „domniemania zgodności" art. 5 ust. 1 lit. b) RODO stanowi jednak, że „dalsze przetwarzanie [...] do celów badań naukowych [...] nie jest uznawane w myśl art. 89 ust. 1 za niezgodne z pierwotnymi celami". Ze względu na jego horyzontalny i złożony charakter temat ten zostanie bardziej szczegółowo omówiony w planowanych wytycznych EROD w sprawie przetwarzania danych dotyczących zdrowia do celów badań naukowych.

44. Art. 89 ust. 1 RODO stanowi, że przetwarzanie danych do celów naukowych „podlega odpowiednim zabezpieczeniom" i że „zabezpieczenia te polegają na wdrożeniu środków technicznych i organizacyjnych zapewniających poszanowanie zasady minimalizacji danych. Środki te mogą też obejmować pseudonimizację danych, o ile pozwala ona realizować powyższe cele".

45. Wymogi określone w art. 89 ust. 1 RODO podkreślają znaczenie zasady minimalizacji danych oraz zasady integralności i poufności, jak również zasady uwzględniania ochrony danych w fazie projektowania i zasady domyślnej ochrony danych (zob. poniżej)[16]. W związku z tym, biorąc pod uwagę wrażliwy charakter danych dotyczących zdrowia oraz ryzyko związane z ponownym wykorzystywaniem danych dotyczących zdrowia do celów badań naukowych, należy podjąć zdecydowane środki w celu zapewnienia odpowiedniego stopnia bezpieczeństwa zgodnie z wymogami art. 32 ust. 1 RODO.

5.3 Minimalizacja danych i ograniczenie przechowywania danych

[15] Wytyczne w sprawie przejrzystości na podstawie rozporządzenia 2016/679 byłej Grupy Roboczej Art. 29 z dnia 11 kwietnia 2018 r., WP260 rev.01, 17/EN, s. 32 (zatwierdzone przez EROD).

[16] Zob. również wytyczne 4/2019 EROD z dnia 13 listopada 2019 r. dotyczące uwzględniania ochrony danych w fazie projektowania i domyślnej ochrony danych (wersja do konsultacji publicznych), dostępne na stronie https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_en

46. W przypadku badań naukowych minimalizację danych można osiągnąć poprzez wymaganie określenia pytań badawczych oraz przeprowadzenia oceny rodzaju i ilości danych niezbędnych do udzielenia właściwej odpowiedzi na te pytania. Rodzaj potrzebnych danych zależy od tego, jaki jest cel badań – nawet jeśli badania mają charakter poszukiwawczy, zawsze powinny być zgodne z zasadą ograniczenia celu zgodnie z art. 5 ust. 1 lit. b) RODO. Co istotne, jeżeli możliwe jest przeprowadzenie badań naukowych z wykorzystaniem danych zanonimizowanych, należy takie dane anonimizować.

47. Ponadto należy ustalić proporcjonalne okresy przechowywania. Jak określono w art. 5 ust. 1 lit. e) RODO, „dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych [...] do celów badań naukowych [...] na mocy art. 89 ust. 1, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą".

48. W celu ustalenia okresów przechowywania (ram czasowych) należy uwzględnić takie kryteria, jak długość i cel badań. Należy zauważyć, że przepisy krajowe również mogą określać zasady dotyczące okresu przechowywania.

5.4 Integralność i poufność

49. Jak wspomniano powyżej, dane wrażliwe – takie jak dane dotyczące zdrowia – zasługują na większą ochronę, ponieważ istnieje większe prawdopodobieństwo, że przetwarzanie takich danych doprowadzi do negatywnych skutków dla osób, których dane dotyczą. Względy te mają w szczególności zastosowanie do pandemii COVID-19, ponieważ przewidywane ponowne wykorzystanie danych dotyczących zdrowia do celów naukowych prowadzi do wzrostu liczby i rodzajów podmiotów przetwarzających takie dane.

50. Należy zauważyć, że zasada integralności i poufności musi być odczytywana w związku z wymogami art. 32 ust. 1 oraz art. 89 ust. 1 RODO. Należy w pełni przestrzegać wspomnianych przepisów. Biorąc pod uwagę wysokie ryzyko, które opisano powyżej, należy zatem wdrożyć odpowiednie i aktualne środki techniczne i organizacyjne w celu zapewnienia wystarczającego poziomu bezpieczeństwa.

51. Środki takie powinny obejmować *co najmniej* pseudonimizację[17], szyfrowanie, umowy o nieujawnianiu informacji, a także ścisły podział ról, ograniczenia ról dostępu i rejestry dostępu. Należy zauważyć, że przepisy krajowe mogą określać konkretne wymogi techniczne lub inne zabezpieczenia, takie jak przestrzeganie zasad tajemnicy zawodowej.

52. Ponadto należy przeprowadzić ocenę skutków dla ochrony danych na mocy art. 35 RODO, jeżeli takie przetwarzanie danych „z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych" zgodnie z art. 35 ust. 1 RODO. Należy uwzględnić wykazy zgodnie z art. 35 ust. 4 i ust. 5 RODO.

53. W tym miejscu EROD podkreśla znaczenie inspektorów ochrony danych. W stosownych przypadkach należy przeprowadzić konsultacje z inspektorami ochrony danych odnośnie do przetwarzania danych dotyczących zdrowia do celów badań naukowych w kontekście pandemii COVID-19.

54. Ponadto przyjęte środki ochrony danych (w tym w trakcie przekazywania danych) powinny być odpowiednio udokumentowane w rejestrze czynności przetwarzania.

[17] Należy zauważyć, że dane osobowe (dotyczące zdrowia), które zostały poddane pseudonimizacji, są nadal uznawane za „dane osobowe" na mocy art. 4 ust. 1 RODO i nie mogą być mylone z „danymi zanonimizowanymi", w przypadku których nie jest już możliwe ustalenie poszczególnych osób, których dane dotyczą. Zob. na przykład motyw 28.

6 WYKONYWANIE PRZEZ OSOBY, KTÓRYCH DANE DOTYCZĄ, PRZYSŁUGUJĄCYCH IM PRAW

55. Co do zasady, sytuacje takie jak obecna pandemia COVID-19 nie zawieszają ani nie ograniczają możliwości wykonywania przez osoby, których dane dotyczą, praw przysługujących im na mocy art. 12–22 RODO. W art. 89 ust. 2 RODO umożliwia się jednak prawodawcy krajowemu ograniczenie (niektórych) praw osoby, której dane dotyczą, określonych w rozdziale 3 tego rozporządzenia. Z tego względu ograniczenia praw osób, których dane dotyczą, *mogą być różne* w zależności od przepisów przyjętych w określonych państwach członkowskich.

56. Ponadto niektóre ograniczenia praw osób, których dane dotyczą – takie jak ograniczenie prawa dostępu na mocy art. 15 ust. 4 RODO oraz ograniczenie prawa do usunięcia danych ustanowione na mocy art. 17 ust. 3 lit. d) RODO – mogą być oparte bezpośrednio na rozporządzeniu. Odstępstwa od obowiązku informacyjnego ustanowionego na mocy art. 14 ust. 5 RODO zostały już omówione powyżej.

57. Należy zauważyć, że w świetle orzecznictwa Trybunału Sprawiedliwości Unii Europejskiej wszelkie ograniczenia praw osób, których dane dotyczą, muszą być stosowane tylko w takim zakresie, w jakim jest to absolutnie konieczne[18].

7 MIĘDZYNARODOWE PRZEKAZYWANIE DANYCH DO CELÓW BADAŃ NAUKOWYCH

58. W kontekście badań naukowych, a w szczególności w kontekście pandemii COVID-19 prawdopodobnie konieczne będzie podjęcie współpracy międzynarodowej, która może skutkować międzynarodowym przekazywaniem danych dotyczących zdrowia do celów badań naukowych poza EOG.

59. W przypadku gdy dane osobowe są przekazywane do państwa lub organizacji międzynarodowej spoza EOG, podmiot przekazujący dane oprócz przestrzegania przepisów określonych w RODO[19], a w szczególności jego art. 5 (zasady ochrony danych), art. 6 (zgodność z prawem) i art. 9 (szczególne kategorie danych osobowych)[20], przestrzega również przepisów rozdziału V (przekazywanie danych)[21].

60. Oprócz standardowego wymogu przejrzystości, o którym mowa na s. 7 niniejszych wytycznych, na podmiocie przekazującym dane spoczywa obowiązek poinformowania osób, których dane dotyczą, o zamiarze przekazania ich danych osobowych do państwa trzeciego lub organizacji międzynarodowej. Dotyczy to między innymi informacji o stwierdzeniu lub braku stwierdzenia przez Komisję Europejską odpowiedniego stopnia ochrony, a także o tym, czy przekazanie danych osobowych odbywa się z zachowaniem właściwych zabezpieczeń opisanych w art. 46 lub na podstawie wyjątku przewidzianego w art. 49 ust. 1. Obowiązek ten istnieje niezależnie od tego, czy dane osobowe zostały uzyskane bezpośrednio od osoby, której dane dotyczą, czy też nie.

[18] Zob. na przykład w odniesieniu do dyrektywy 95/46/WE wyrok Trybunału Sprawiedliwości z dnia 14 lutego 2019 r., sprawa C-345/17 (Buivids), pkt 64.
[19] Art. 44 RODO.
[20] Zob. sekcje 4–6 niniejszych wytycznych.
[21] Zob. również wytyczne 2/2018 EROD z dnia 25 maja 2018 r. w sprawie wyjątków określonych w art. 49 rozporządzenia 2016/679, s. 3, odnośnie do spełnienia dwóch warunków, dostępne na stronie internetowej https://edpb.europa.eu/our-work-tools/our-documents/smjernice/guidelines-22018-derogations-article-49-under-regulation_pl

61. Ogólnie rzecz biorąc, podczas wypracowywania rozwiązań pozwalających spełnić wspomniane warunki przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych podmioty przekazujące dane powinny ocenić zagrożenia dla praw i wolności osób, których dane dotyczą, przy każdym przekazaniu danych[22], opowiadając się za takimi rozwiązaniami, które gwarantują ciągłą ochronę podstawowych praw tych osób i zabezpieczeń w zakresie przetwarzania ich danych, nawet po ich przekazaniu. Taka sytuacja będzie miała miejsce w przypadku przekazywania danych do państw o odpowiednim poziomie ochrony[23] lub w przypadku zastosowania jednego z odpowiednich zabezpieczeń opisanych w art. 46 RODO[24], zapewniając egzekwowalne prawa osób, których dane dotyczą, i skuteczne środki ochrony prawnej.

62. W przypadku braku decyzji stwierdzającej odpowiednie stopień ochrony na mocy art. 45 ust. 3 RODO lub braku odpowiednich zabezpieczeń opisanych w art. 46 RODO, w art. 49 RODO przewidziano pewne szczególne sytuacje, w których przekazywanie danych osobowych może odbywać się w drodze odstępstwa. Wyjątki przewidziane w art. 49 RODO są zatem odstępstwami od zasady ogólnej i w związku z tym powinny być interpretowane w sposób zawężający i osobno dla poszczególnych przypadków[25]. W odniesieniu do obecnego kryzysu COVID-19 mogą mieć zastosowanie przepisy art. 49 ust. 1 lit. d) („przekazanie jest niezbędne ze względu na ważne względy interesu publicznego") oraz lit. a) („wyraźna zgoda").

63. Pandemia COVID-19 spowodowała kryzys sanitarny o niespotykanym dotąd charakterze i nadzwyczajnej skali. W tym kontekście EROD uważa, że UE i większość jej państw członkowskich uznały walkę z COVID-19 za ważny interes publiczny[26], który może wymagać pilnych działań w dziedzinie badań naukowych (na przykład w celu określenia metod leczenia lub opracowania szczepionek), a także wiązać się z przekazywaniem danych do państw trzecich lub organizacji międzynarodowych[27].

64. W obecnym kontekście pandemii na wspomniany wyżej wyjątek mogłyby powołać się nie tylko organy publiczne, ale również podmioty prywatne pełniące rolę w realizacji takiego interesu publicznego (na przykład instytut badawczy uniwersytetu współpracujący przy opracowaniu szczepionki w ramach międzynarodowego partnerstwa).

[22] Międzynarodowe przekazywanie danych może stanowić czynnik ryzyka, który należy uwzględnić przy przeprowadzaniu oceny skutków dla ochrony danych, o której mowa na s. 10 niniejszych wytycznych.
[23] Wykaz krajów uznanych za odpowiednie przez Komisję Europejską jest dostępny pod adresem https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en
[24] Na przykład standardowe klauzule ochrony danych na mocy art. 46 ust. 2 lit. c) lub d) RODO, klauzule umowne *ad-hoc* na mocy art. 46 ust. 3 lit. a) RODO lub uzgodnienia administracyjne na mocy art. 46 ust. 3 lit. b) RODO.
[25] Zob. wytyczne 2/2018, s. 3.
[26] Art. 168 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE) stanowi, że wysoki poziom ochrony zdrowia ludzkiego jest ważnym celem przy określaniu i urzeczywistnianiu wszystkich polityk i działań Unii. Na tej podstawie działania Unii stanowią wsparcie polityk krajowych mające na celu poprawę zdrowia publicznego, w tym walkę z epidemią i poważnymi transgranicznymi zagrożeniami dla zdrowia, np. poprzez wspieranie badań nad ich przyczynami, sposobami ich rozprzestrzeniania się oraz zapobiegania tym zagrożeniom. Z tego samego względu w motywach 46 i 112 RODO odniesiono się do przetwarzania przeprowadzanego w kontekście walki z epidemiami jako do przykładu przetwarzania służącego ważnemu interesowi publicznemu. W kontekście pandemii COVID-19 Unia przyjęła szereg środków w wielu różnych obszarach (np. finansowanie systemów opieki zdrowotnej, wsparcie dla pacjentów transgranicznych i rozmieszczanie personelu medycznego, pomoc finansowa dla najbardziej potrzebujących osób, transport, wyroby medyczne itp.), opierając się na założeniu, że UE stoi w obliczu poważnej sytuacji zagrożenia zdrowia publicznego, która wymaga pilnej reakcji.
[27] EROD podkreśla, że w motywie 112 RODO przytoczono międzynarodową wymianę danych pomiędzy właściwymi służbami do celów zdrowia publicznego jako przykład zastosowania tego wyjątku.

65. Ponadto w niektórych sytuacjach, w szczególności gdy dane są przekazywane przez podmioty prywatne na potrzeby badań medycznych mających na celu zwalczanie pandemii COVID-19[28], takie przekazywanie danych osobowych mogłoby również odbywać się w oparciu o wyraźną zgodę osób, których dane dotyczą[29].

66. W obecnym kontekście pandemii – gdy niemożliwe jest oparcie się na decyzji stwierdzającej odpowiedni stopień ochrony na mocy art. 45 ust. 3 lub na odpowiednich zabezpieczeniach na mocy art. 46 – organy publiczne i podmioty prywatne mogą oprzeć się na mających zastosowanie wyjątkach, o których mowa powyżej, traktując je przede wszystkim jako środek tymczasowy ze względu na pilność sytuacji medycznej na świecie.

67. Jeżeli charakter kryzysu COVID-19 może stanowić w tym kontekście uzasadnienie do wykorzystania mających zastosowanie wyjątków w odniesieniu do początkowego przekazywania danych do celów badawczych, to już powtarzające się przekazywanie danych do państw trzecich w ramach długotrwałego projektu badawczego w tym zakresie musiałoby zostać ujęte w ramach odpowiednich zabezpieczeń zgodnie z art. 46 RODO[30].

68. Należy ponadto zauważyć, że w poszczególnych przypadkach takiego przekazania należy uwzględnić odpowiednie role (administratora, podmiotu przetwarzającego, współadministratora) i związane z nimi obowiązki zaangażowanych podmiotów (sponsora, badacza) w celu określenia odpowiednich środków służących do opracowania struktury przekazywania danych.

8 PODSUMOWANIE

69. Najważniejsze ustalenia niniejszych wytycznych są następujące:

    1. W RODO przewidziano szczególne przepisy w zakresie przetwarzania danych dotyczących zdrowia do celów badań naukowych, które mają również zastosowanie w kontekście pandemii COVID-19.
    2. Prawodawca krajowy każdego państwa członkowskiego może przyjąć szczególne przepisy zgodnie z art. 9 ust. 2 lit. i) oraz lit. j) RODO, aby umożliwić przetwarzanie danych dotyczących zdrowia do celów badań naukowych. Przetwarzanie danych dotyczących zdrowia do celów badań naukowych musi być również objęte jedną z podstaw prawnych określonych w art. 6 ust. 1 RODO. W związku z tym warunki i zakres takiego przetwarzania różnią się w zależności od przepisów przyjętych w danym państwie członkowskim.
    3. Wszystkie przyjęte przepisy na podstawie art. 9 ust. 2 lit. i) oraz lit. j) RODO muszą być interpretowane w świetle zasad określonych na mocy art. 5 RODO i z uwzględnieniem orzecznictwa Trybunału Sprawiedliwości Unii Europejskiej. W szczególności wyjątki i ograniczenia w związku z ochroną danych przewidziane w art. 9 ust. 2 lit. j) i art. 89 ust. 2 RODO muszą być stosowane tylko w takim zakresie, w jakim jest to bezwzględnie niezbędne.
    4. Biorąc pod uwagę zagrożenia związane z przetwarzaniem danych w kontekście pandemii COVID-19, należy położyć duży nacisk na zgodność z przepisami art. 5 ust. 1 lit. f), art. 32 ust. 1 i art. 89 ust. 1 RODO. Jeśli występuje konieczność przeprowadzenia oceny skutków dla ochrony danych zgodnie z art. 35 RODO, należy dokonać takiej oceny.

[28] Jak określono w art. 49 ust. 3 RODO, zgoda nie może być wykorzystywana do realizowania działań prowadzonych przez organy publiczne w ramach wykonywania przysługujących im uprawnień publicznych.
[29] Zob. wytyczne EROD 2/2018, sekcja 2.1.
[30] Zob. wytyczne EROD 2/2018, s. 5.

5. Należy ustalić proporcjonalne okresy przechowywania (ramy czasowe). W celu określenia takich okresów przechowywania należy uwzględnić takie kryteria, jak długość i cel badań. Również przepisy krajowe mogą określać zasady dotyczące okresu przechowywania, w związku z czym należy je wziąć pod uwagę.
6. Co do zasady, sytuacje takie jak obecna pandemia COVID-19 nie zawieszają ani nie ograniczają możliwości wykonywania przez osoby, których dane dotyczą, praw przysługujących im na mocy art. 12–22 RODO. W art. 89 ust. 2 RODO umożliwia się jednak prawodawcy krajowemu ograniczenie (niektórych) praw osoby, której dane dotyczą, określonych w rozdziale 3 RODO. Z tego względu ograniczenia praw osób, których dane dotyczą, *mogą być różne* w zależności od przepisów przyjętych w określonych państwach członkowskich.
7. Jeżeli chodzi o międzynarodowe przekazywanie danych, w przypadku braku decyzji stwierdzającej odpowiedni stopień ochrony na mocy art. 45 ust. 3 RODO lub braku odpowiednich zabezpieczeń opisanych w art. 46 RODO, organy publiczne i podmioty prywatne mogą polegać na mających zastosowanie wyjątkach zgodnie z art. 49 RODO. Wyjątki przewidziane w art. 49 RODO mają jednak wyłącznie charakter odstępstwa.

W imieniu Europejskiej Rady Ochrony Danych

Przewodnicząca

(Andrea Jelinek)



Wytyczne 2/2020 w sprawie art. 46 ust. 2 lit. a) i art. 46 ust. 3 lit. b) rozporządzenia 2016/679 dotyczącego przekazywania danych osobowych między organami i podmiotami publicznymi z EOG i spoza EOG

Wersja 2.0

przyjęte 15 grudnia 2020 r.

Historia wersji

Wersja 2.0	15 grudnia 2020 r.	Przyjęcie wytycznych po konsultacjach publicznych
Wersja 1.0	18 lutego 2020 r.	Przyjęcie wytycznych do konsultacji publicznych

Spis treści

1 Uwagi ogólne ... 6
1.1 Cel ... 6
1.2 Zasady ogólne mające zastosowanie do międzynarodowego przekazywania danych ... 7
1.3 Definicja organu lub podmiotu publicznego ... 7
2 Ogólne zalecenia dotyczące odpowiednich zabezpieczeń zapewnianych na mocy art. 46 ust. 2 lit. a) i art. 46 ust. 3 lit. b) RODO ... 8
2.1 Cel i zakres ... 9
2.2 Definicje ... 9
2.3 Zasady ochrony danych ... 9
2.3.1 Zasada ograniczenia celu ... 9
2.3.2 Zasady prawidłowości i minimalizacji danych ... 10
2.3.3 Zasada ograniczenia przechowywania ... 10
2.3.4 Bezpieczeństwo i poufność danych ... 10
2.4 Prawa osób, których dane dotyczą ... 11
2.4.1 Prawo do przejrzystości ... 11
2.4.2 Prawo dostępu do danych, ich sprostowania, usunięcia i ograniczenia przetwarzania danych oraz prawo do sprzeciwu ... 12
2.4.3 Zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach ... 13
2.4.4 Prawo dochodzenia roszczeń ... 13
2.4.5 Ograniczenia praw osób, których dane dotyczą ... 13
2.5 Ograniczenia dotyczące dalszego przekazywania i udostępniania danych (w tym ujawniania i dostępu administracji rządowej) ... 13
2.6 Dane wrażliwe ... 15
2.7 Mechanizmy zaskarżenia ... 15
2.8 Mechanizmy nadzoru ... 18
2.9 Klauzula regulująca rozwiązanie umowy ... 19
3 Szczegółowe informacje na temat art. 46 RODO ... 20
3.1 Szczegółowe informacje na temat prawnie wiążących i egzekwowalnych instrumentów – art. 46 ust. 2 lit. a) RODO ... 20
3.2 Szczegółowe informacje na temat uzgodnień administracyjnych – art. 46 ust. 3 lit. b) RODO 20
4 Pytania dotyczące kwestii proceduralnych ... 22

Europejska Rada Ochrony Danych,

uwzględniając art. 70 ust. 1 lit. e) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (zwanego dalej „RODO"),

uwzględniając Porozumienie EOG, w szczególności załącznik XI i protokół 37 do tego Porozumienia, zmienione decyzją Wspólnego Komitetu EOG nr 154/2018 z dnia 6 lipca 2018 r.[1],

uwzględniając art. 12 i 22 swojego regulaminu wewnętrznego,

PRZYJĘŁA NASTĘPUJĄCE WYTYCZNE:

[1] Odniesienia do „państw członkowskich" zawarte w niniejszych wytycznych należy rozumieć jako odniesienia do „państw należących do EOG".

1 UWAGI OGÓLNE

1.1 Cel

1. Niniejszy dokument ma na celu przedstawienie wytycznych dotyczących stosowania art. 46 ust. 2 lit. a) i art. 46 ust. 3 lit. b) ogólnego rozporządzenia o ochronie danych (RODO) w odniesieniu do przekazywania danych osobowych przez organy lub podmioty publiczne z EOG (zwane dalej „podmiotami publicznymi") do podmiotów publicznych w państwach trzecich lub organizacji międzynarodowych w zakresie, w jakim te podmioty lub organizacje nie są objęte przyjętą przez Komisję Europejską decyzją stwierdzającą odpowiedni stopień ochrony danych [2]. Podmioty publiczne mogą zdecydować się na skorzystanie z tych mechanizmów, które uznano w RODO za bardziej odpowiednie do ich sytuacji, ale mają również możliwość korzystania z innych stosownych narzędzi zapewniających odpowiednie zabezpieczenia zgodnie z art. 46 RODO.

2. Celem wytycznych jest przedstawienie oczekiwań Europejskiej Rady Ochrony Danych (EROD) w kwestii zabezpieczeń, które należy wprowadzić za pomocą prawnie wiążącego i egzekwowalnego instrumentu między podmiotami publicznymi zgodnie z art. 46 ust. 2 lit. a) RODO, lub pod warunkiem uzyskania zezwolenia właściwego organu nadzorczego za pomocą postanowień uzgodnień administracyjnych między podmiotami publicznymi zgodnie z art. 46 ust. 3 lit. b) RODO[3]. EROD zdecydowanie zaleca, aby strony stosowały wytyczne jako punkt odniesienia na wczesnym etapie, gdy planują podpisanie lub zmianę takich instrumentów lub uzgodnień[4].

3. Wytyczne należy odczytywać w związku z innymi wcześniejszymi pracami EROD (w tym z dokumentami zatwierdzonymi przez podmiot będący jej poprzednikiem, Grupę Roboczą Art. 29[5]) na temat głównych kwestii dotyczących zakresu terytorialnego i przekazywania danych osobowych do państw trzecich[6]. Wytyczne zostaną poddane przeglądowi i, w razie konieczności, zaktualizowane w oparciu o praktyczne doświadczenia zdobyte w wyniku stosowania RODO.

4. Niniejsze wytyczne obejmują międzynarodowe przekazywanie danych między podmiotami publicznymi odbywające się w różnych celach związanych ze współpracą administracyjną wchodzących w zakres RODO. W związku i zgodnie z art. 2 ust. 2 RODO wytyczne te nie obejmują przekazywania danych w obszarze bezpieczeństwa publicznego, obrony lub bezpieczeństwa państwa. Nie dotyczą one również przetwarzania i przekazywania danych przez właściwe organy w celu ścigania przestępstw, ponieważ takie przetwarzanie i przekazywanie danych jest regulowane odrębnym szczegółowym instrumentem prawnym– dyrektywą 2016/680[7]. Ponadto, w wytycznych skoncentrowano się

[2] Na przykład japońskie podmioty publiczne, które nie są objęte decyzją stwierdzającą odpowiedni stopień ochrony w Japonii, ponieważ dotyczy ona wyłącznie organizacji sektora prywatnego.
[3] W niniejszych wytycznych termin „umowy międzynarodowe" oznacza prawnie wiążące i egzekwowalne instrumenty, o których mowa w art. 46 ust. 2 lit. a) RODO, oraz uzgodnienia administracyjne, o których mowa w art. 46 ust. 3 lit. b) RODO.
[4] Art. 96 RODO stanowi, że umowy, które zostały zawarte przed 24 maja 2016 r., pozostają w mocy do czasu ich zmiany, zastąpienia lub uchylenia.
[5] Grupa robocza ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych ustanowiona na mocy art. 29 dyrektywy o ochronie danych 95/46/WE.
[6] Zob. dokument Grupy Roboczej Art. 29 zatytułowany „Odpowiedni stopień ochrony przekazywanych danych osobowych" (WP 254 rev. 01, zatwierdzony przez EROD w dniu 25 maja 2018 r.), wytyczne EROD 2/2018 w sprawie wyjątków określonych w art. 49 rozporządzenia 2016/679 oraz wytyczne EROD 3/2018 w sprawie terytorialnego zakresu stosowania RODO (art. 3).
[7] Dyrektywa (UE) 2016/680 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości,

wyłącznie na przekazywaniu danych między podmiotami publicznymi i nie obejmują one przekazywania danych osobowych z podmiotu publicznego do podmiotu prywatnego lub z podmiotu prywatnego do podmiotu publicznego.

1.2 Zasady ogólne mające zastosowanie do międzynarodowego przekazywania danych

5. Zgodnie z art. 44 RODO podmiot przekazujący dane osobowe do państw trzecich lub organizacji międzynarodowych musi nie tylko przestrzegać przepisów zawartych w rozdziale V RODO, ale również spełniać warunki określone w pozostałych przepisach RODO. W szczególności każda czynność przetwarzania musi być zgodna z zasadami ochrony danych określonymi w art. 5 RODO, zgodna z prawem, jak określono w art. 6 RODO, oraz zgodna z art. 9 RODO w przypadku szczególnych kategorii danych. W związku z tym każda czynność musi spełniać dwa warunki: po pierwsze, podstawa prawna musi mieć zastosowanie do przetwarzania danych jako takiego wraz ze wszystkimi właściwymi przepisami RODO; a po drugie, należy przestrzegać przepisów rozdziału V RODO.

6. Art. 46 RODO stanowi, że „w razie braku decyzji na mocy art. 45 ust. 3 administrator lub podmiot przetwarzający mogą przekazać dane osobowe do państwa trzeciego lub organizacji międzynarodowej wyłącznie, gdy zapewnią odpowiednie zabezpieczenia, i pod warunkiem, że dostępne są egzekwowalne prawa osób, których dane dotyczą oraz skuteczne środki ochrony prawnej." Takie odpowiednie zabezpieczenia można zapewnić za pomocą prawnie wiążącego i egzekwowalnego instrumentu między podmiotami publicznymi (art. 46 ust. 2 lit. a) RODO) lub – pod warunkiem uzyskania zezwolenia właściwego organu nadzorczego – za pomocą postanowień uzgodnień administracyjnych między podmiotami publicznymi, w których przewidziane będą skuteczne i egzekwowalne prawa osób, których dane dotyczą (art. 46 ust. 3 lit. b) RODO). Jak wyjaśnił Trybunał Sprawiedliwości Unii Europejskiej (TSUE), takie odpowiednie zabezpieczenia powinny gwarantować, by prawa przysługujące osobom, których dane są przekazywane, korzystały ze stopnia ochrony merytorycznie równoważnego temu gwarantowanemu w EOG[8].

7. Niezależnie od tego rozwiązania jak i w przypadku jego niestosowania, w art. 49 RODO określono również ograniczoną liczbę szczególnych sytuacji, w których międzynarodowe przekazywanie danych może mieć miejsce, w przypadku braku stwierdzenia przez Komisję Europejską zapewniania odpowiedniego poziomu ochrony[9]. W szczególności jeden z wyjątków dotyczy przekazania niezbędnego ze względu na ważne względy interesu publicznego uznanego w prawie Unii lub w prawie państwa członkowskiego, któremu podlega administrator, w tym w duchu zasady wzajemności w ramach współpracy międzynarodowej[10]. Jak jednak wyjaśniono w poprzednich opublikowanych przez EROD wytycznych, wyjątki przewidziane w art. 49 RODO należy interpretować w sposób zawężający i muszą one dotyczyć głównie przetwarzania, które jest sporadyczne i niepowtarzające się[11].

1.3 Definicja organu lub podmiotu publicznego

8. W RODO nie zdefiniowano pojęcia „organ lub podmiot publiczny". EROD uważa, że pojęcie to jest wystarczająco szerokie, aby mogło objąć zarówno podmioty publiczne w państwach trzecich, jak i organizacje międzynarodowe[12]. W przypadku podmiotów publicznych w państwach trzecich pojęcie to należy rozumieć zgodnie z prawem krajowym. W związku z tym do podmiotów publicznych zaliczają się organy rządowe różnych szczebli (np. władze krajowe, regionalne i lokalne), ale mogą to być również inne podmioty prawa publicznego (np. agencje wykonawcze, uniwersytety, szpitale itp.)[13]. Zgodnie z art. 4 pkt 26 RODO „organizacja międzynarodowa" oznacza organizację i organy jej podlegające działające na podstawie prawa międzynarodowego publicznego lub inny organ powołany w drodze umowy między co najmniej dwoma państwami lub na podstawie takiej umowy.

9. EROD przypomina, że RODO stosuje się, nie naruszając przepisów prawa międzynarodowego, takich jak przepisy regulujące przywileje i immunitety organizacji międzynarodowych. Jednocześnie należy pamiętać, że każdy podmiot publiczny z EOG przekazujący dane organizacjom międzynarodowym musi przestrzegać przepisów RODO dotyczących przekazywania danych do państw trzecich lub organizacji międzynarodowych[14].

2 OGÓLNE ZALECENIA DOTYCZĄCE ODPOWIEDNICH ZABEZPIECZEŃ ZAPEWNIANYCH NA MOCY ART. 46 UST. 2 LIT. a) I ART. 46 UST. 3 LIT. b) RODO

10. W przeciwieństwie do art. 26 ust. 2 dyrektywy 95/46/WE w art. 46 RODO przewidziano dodatkowe odpowiednie zabezpieczenia jako narzędzia przekazywania danych między podmiotami publicznymi, mianowicie:

    (i) prawnie wiążący i egzekwowalny instrument, zgodnie z art. 46 ust. 2 lit. a) RODO, lub
    (ii) postanowienia uzgodnień administracyjnych, zgodnie z art. 46 ust. 3 lit. b) RODO.

    Takie instrumenty i uzgodnienia mogą mieć charakter dwustronny lub wielostronny.

11. W poniższej sekcji przedstawiono pewne ogólne zalecenia, które mają pomóc w zapewnieniu zgodności z RODO prawnie wiążących instrumentów lub uzgodnień administracyjnych (zwanych dalej „umowami międzynarodowymi") między podmiotami publicznymi.

12. Chociaż art. 46 i motyw 108 RODO nie zawierają konkretnych wskazówek dotyczących gwarancji, które należy zawrzeć w takich umowach międzynarodowych, uwzględniając art. 44 RODO[15] i najnowsze orzecznictwo TSUE[16], EROD opracowała wykaz minimalnych zabezpieczeń, które należy zawrzeć w umowach międzynarodowych między podmiotami publicznymi objętymi zakresem art. 46 ust. 2 lit. a) lub art. 46 ust. 3 lit. b) RODO. Zabezpieczenia te mają na celu zapewnienie, aby nie został naruszony stopień ochrony osób fizycznych przewidziany w RODO, gdy ich dane osobowe są

prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych.
[8] Wyrok TSUE w sprawie C-311/18, Data Protection Commissioner/Facebook Ireland Ltd i Maximillian Schrems („Schrems II"), pkt 96.
[9] Więcej informacji na temat art. 49 i jego wzajemnej zależności z art. 46 można znaleźć w Wytycznych EROD 2/2018 w sprawie wyjątków określonych w art. 49 rozporządzenia 2016/679.
[10] Zob. Wytyczne EROD 2/2018 w sprawie wyjątków określonych w art. 49 rozporządzenia 2016/679, s. 10.
[11] Zob. Wytyczne EROD w sprawie wyjątków określonych w art. 49 rozporządzenia 2016/679, s. 5.

[12] Zob. również motyw 108 RODO.
[13] Zob. np. definicje „organu sektora publicznego" „podmiotu prawa publicznego" w art. 2 pkt 1 i 2 dyrektywy 2003/98/WE Parlamentu Europejskiego i Rady z 17 listopada 2003 r. w sprawie ponownego wykorzystywania informacji sektora publicznego (Dz.U. L 345 z 31.12.2003, s. 90).
[14] Zob. Wytyczne EROD 3/2018 w sprawie terytorialnego zakresu stosowania RODO, s. 23.
[15] Art. 44 RODO stanowi: „Wszystkie przepisy niniejszego rozdziału należy stosować z myślą o zapewnieniu, by nie został naruszony stopień ochrony osób fizycznych zagwarantowany w niniejszym rozporządzeniu."
[16] Wyrok TSUE z 16 lipca 2020 r. w sprawie C-311/18, Data Protection Commissioner/Facebook Ireland Ltd i Maximillian Schrems („Schrems II").

przekazywane poza EOG, oraz aby stopień ochrony osób, których dane dotyczą, był merytorycznie równoważny temu zagwarantowanemu w UE przez RODO[17].

13. Zgodnie z najnowszym orzecznictwem TSUE[18] obowiązkiem przekazującego podmiotu publicznego w państwie członkowskim jest przeprowadzenie oceny, w razie potrzeby z pomocą otrzymującego podmiotu publicznego, czy w państwie trzecim zachowany jest stopień ochrony wymagany prawem Unii, celem ustalenia, czy przestrzeganie wykazu zabezpieczeń zawartego w umowie międzynarodowej będzie możliwe w praktyce, uwzględniając ewentualny wpływ prawodawstwa państwa trzeciego na przestrzeganie tych zabezpieczeń.

14. W tym względzie należy również zauważyć, że w celu zagwarantowania zabezpieczeń wymienionych w niniejszych wytycznych, umowy międzynarodowe mogą opierać się na już istniejących elementach prawa krajowego państwa trzeciego lub na przepisach wewnętrznych/ramach regulacyjnych organizacji międzynarodowej.

2.1 Cel i zakres

15. W umowach międzynarodowych należy zdefiniować ich zakres, a cele tych umów należy określić jednoznacznie i szczegółowo. Ponadto, należy jasno określić kategorie danych osobowych, których umowy te dotyczą, oraz rodzaj przetwarzania danych osobowych, które są przekazywane i przetwarzane na podstawie umowy.

2.2 Definicje

16. Umowy międzynarodowe powinny zawierać zgodne z RODO definicje podstawowych pojęć i praw dotyczących danych osobowych, które są istotne dla danej umowy. Przykładowo, takie umowy powinny zawierać definicje następujących istotnych terminów, jeżeli takie terminy w nich występują: „dane osobowe", „przetwarzanie danych osobowych", „administrator danych", „podmiot przetwarzający", „odbiorca" i „dane wrażliwe".

2.3 Zasady ochrony danych

17. Umowy międzynarodowe muszą zawierać konkretne sformułowania zobowiązujące obie strony do zapewnienia przestrzegania podstawowych zasad ochrony danych.

2.3.1 Zasada ograniczenia celu

18. W umowach międzynarodowych należy określić cele, w których dane osobowe mają być przekazywane i przetwarzane, w tym cele dalszego przetwarzania zgodne z celami, w których dane osobowe zostały pierwotnie zebrane, a także należy w nich zapewnić, aby dane nie były przetwarzane dalej w celach niezgodnych z pierwotnymi celami. Cele zgodne z pierwotnymi celami mogą obejmować przechowywanie danych do celów archiwalnych w interesie publicznym, jak również przetwarzanie danych do celów badań naukowych lub historycznych lub do celów statystycznych. Dla większej jasności zaleca się, by konkretne cele przetwarzania i przekazywania danych zostały wymienione w treści umowy międzynarodowej.

[17] Wyrok TSUE z 16 lipca 2020 r. w sprawie C-311/18, Data Protection Commissioner/Facebook Ireland Ltd i Maximillian Schrems („Schrems II"), pkt 105.
[18] Tamże.

19. Aby uniknąć ryzyka „zmiany celu", w takich umowach należy również sprecyzować, że przekazywanych danych nie można wykorzystywać do żadnych innych celów niż te wyraźnie wymienione w umowie, z wyjątkiem przypadków określonych w poniższym punkcie.

20. Jeżeli obie strony umowy międzynarodowej chcą zezwolić otrzymującemu podmiotowi publicznemu na inne, zgodne z przepisami wykorzystywanie przekazanych danych osobowych, dalsze wykorzystywanie przez otrzymujący podmiot publiczny jest dozwolone jedynie wtedy, gdy jest zgodne z pierwotnym wykorzystywaniem i zostało wcześniej zgłoszone przekazującemu podmiotowi publicznemu, który może wyrazić sprzeciw z określonych powodów.

2.3.2 Zasady prawidłowości i minimalizacji danych

21. Umowa międzynarodowa musi określać, że przekazywane i dalej przetwarzane dane muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przekazywane i dalej przetwarzane.

22. W praktyce istotnym celem tej zasady minimalizacji danych jest uniknięcie przekazywania danych osobowych, gdy są one nieadekwatne lub nadmierne.

23. Ponadto, dane powinny być prawidłowe i aktualne, z uwzględnieniem celów, w których są przetwarzane. Umowa międzynarodowa musi zatem stanowić, że strona przekazująca zapewni, aby dane osobowe przekazywane na mocy umowy były prawidłowe i, w stosownych przypadkach, aktualne. Ponadto umowa powinna stanowić, że jeżeli jedna ze stron zauważy, że przekazano lub przetwarza się nieprawidłowe lub nieaktualne dane, musi bezzwłocznie powiadomić o tym drugą stronę. Ponadto umowa powinna zapewniać, aby w przypadku potwierdzenia, że przekazane lub przetwarzane dane są nieprawidłowe, każda ze stron przetwarzających dane podjęła wszelkie zasadne działania w celu sprostowania lub usunięcia tych informacji.

2.3.3 Zasada ograniczenia przechowywania

24. Strony muszą zapewnić, aby umowa międzynarodowa zawierała klauzulę dotyczącą zatrzymywania danych. W klauzuli tej należy w szczególności sprecyzować, że danych osobowych nie zatrzymuje się na czas nieokreślony, ale przechowuje się je w formie umożliwiającej identyfikację osób, których dane dotyczą, jedynie przez okres niezbędny do celów, w których dane te zostały przekazane, a następnie przetwarzane. Może to obejmować przechowywanie danych tak długo, jak jest to konieczne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, pod warunkiem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne w celu ochrony praw i wolności osób, których dane dotyczą, takie jak dodatkowe środki techniczne (np. środki bezpieczeństwa, pseudonimizacja) i ograniczenia dostępu. Jeżeli w prawodawstwie krajowym lub w przepisach wewnętrznych/ramach regulacyjnych organizacji międzynarodowej nie określono jeszcze maksymalnego okresu zatrzymywania, należy go określić w tekście umowy.

2.3.4 Bezpieczeństwo i poufność danych

25. Strony powinny zobowiązać się do zapewnienia bezpieczeństwa i poufności prowadzonego przez siebie przetwarzania i przekazywania danych osobowych.
W szczególności strony powinny zobowiązać się do wprowadzenia odpowiednich środków technicznych i organizacyjnych w celu ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem dostępem, zniszczeniem, utratą, modyfikacją lub nieuprawnionym ujawnieniem. Środki te mogą obejmować na przykład szyfrowanie, w tym w trakcie przekazywania,

pseudonimizację, oznaczanie informacji jako danych osobowych przekazywanych z EOG, ograniczenie zakresu osób mających dostęp do danych osobowych, zapewnienie bezpiecznego przechowywania danych osobowych lub wdrożenie zasad mających na celu zapewnienie, aby dane osobowe były przechowywane w sposób bezpieczny i poufny.
Poziom bezpieczeństwa powinien uwzględniać zagrożenia, stan wiedzy technicznej oraz związane z tym koszty.

26. Umowa międzynarodowa może ponadto stanowić, że jeśli jedna ze stron dowie się o naruszeniu ochrony danych osobowych, poinformuje o tym jak najszybciej drugą stronę (lub pozostałe strony) oraz zastosuje rozsądne i odpowiednie środki w celu zaradzenia naruszeniu ochrony danych osobowych i zminimalizowania potencjalnych niekorzystnych skutków, w tym poprzez zawiadomienie bez zbędnej zwłoki osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, jeśli to naruszenie ochrony danych osobowych może spowodować wysokie ryzyko naruszenia praw i wolności osoby fizycznej.
Zaleca się, aby w umowie międzynarodowej określono termin zgłoszenia naruszenia ochrony danych osobowych, a także procedury zawiadomienia osoby, której dane dotyczą.

2.4 Prawa osób, których dane dotyczą

27. Umowa międzynarodowa musi gwarantować egzekwowalne i skuteczne prawa osób, których dane dotyczą, jak określono w art. 46 ust. 1 i motywie 108 RODO.

28. W umowie należy wymienić prawa przysługujące osobom, których dane dotyczą, w tym konkretne zobowiązania podjęte przez strony w celu zapewnienia takich praw. Aby umowa międzynarodowa była skuteczna, musi przewidywać mechanizmy zapewniające stosowanie ich w praktyce. Ponadto każde naruszenie praw osób, których dane dotyczą, musi pociągać za sobą odpowiedni środek zaradczy.

2.4.1 Prawo do przejrzystości

29. Strony muszą zadbać o to, aby umowa międzynarodowa zawierała jasne sformułowania opisujące obowiązki stron w zakresie przejrzystości.

30. Obowiązki te powinny obejmować m.in. ogólną informację wskazującą co najmniej, jak i dlaczego podmioty publiczne mogą przetwarzać i przekazywać dane osobowe, dane narzędzie wykorzystywane do przekazywania danych, podmioty, do których dane te można przekazywać, prawa przysługujące osobom, których dane dotyczą, i obowiązujące ograniczenia, dostępne mechanizmy zaskarżenia oraz dane kontaktowe służące do zgłaszania sporów lub roszczeń.

31. Należy jednak pamiętać, że w przypadku przekazującego podmiotu publicznego nie wystarczy ogólna informacja umieszczona na stronie internetowej tego podmiotu publicznego. Przekazujący podmiot publiczny powinien podawać odpowiednie informacje każdej osobie, której dane dotyczą, zgodnie z obowiązkami informacyjnymi określonymi w art. 13 i 14 RODO[19].
W umowie międzynarodowej można również wskazać pewne wyjątki od podawania takich informacji. Wyjątki te są ograniczone i powinny być zgodne z wyjątkami przewidzianymi w art. 14 ust. 5 RODO – na przykład mogą dotyczyć sytuacji, w której osoba, której dane dotyczą, dysponuje już tymi informacjami lub gdy udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku.

[19] Zob. Wytyczne EROD w sprawie przejrzystości na podstawie rozporządzenia 2016/679, GR 260 rev. 01, s. 13–22.

32. Strony muszą się zobowiązać do udostępnienia umowy międzynarodowej osobom, których dane dotyczą, na ich wniosek oraz do podania umowy międzynarodowej lub odpowiednich postanowień przewidujących odpowiednie zabezpieczenia do wiadomości publicznej na swojej stronie internetowej. W zakresie niezbędnym do ochrony informacji szczególnie chronionych lub innych informacji poufnych, przed przekazaniem kopii umowy lub jej publicznym udostępnieniem, z tekstu umowy międzynarodowej można usunąć odpowiednie informacje. W stosownych przypadkach, aby umożliwić osobie, której dane dotyczą, zrozumienie treści umowy międzynarodowej, strony muszą przedstawić zrozumiałe streszczenie tej umowy.

2.4.2 Prawo dostępu do danych, ich sprostowania, usunięcia i ograniczenia przetwarzania danych oraz prawo do sprzeciwu

33. Umowa międzynarodowa powinna zabezpieczać prawo osoby, której dane dotyczą, do uzyskania informacji o wszystkich przetwarzanych danych osobowych, które jej dotyczą, i dostępu do tych danych, prawo do sprostowania i usunięcia tych danych, prawo do ograniczenia przetwarzania danych oraz, w stosownych przypadkach, prawo do sprzeciwu wobec przetwarzania danych z przyczyn związanych z jej szczególną sytuacją.

34. W kwestii prawa dostępu, w umowie międzynarodowej należy sprecyzować, że osoby fizyczne są uprawnione do uzyskania od otrzymującego podmiotu publicznego potwierdzenia, czy przetwarzane są dane osobowe, które ich dotyczą, a jeżeli ma to miejsce, są uprawnione do uzyskania dostępu do tych danych; a także do uzyskania konkretnych informacji dotyczących przetwarzania, takich jak cel przetwarzania, kategorie przetwarzanych danych osobowych, odbiorcy, którym dane osobowe są ujawniane, przewidywany okres przechowywania i dostępne środki zaskarżenia.

35. W umowie należy ponadto wskazać, kiedy można powołać się na te prawa, oraz określić tryb wykonywania praw przez osoby, których dane dotyczą, wobec obu stron, a także sposób postępowania stron w przypadku otrzymania takich wniosków. Na przykład w odniesieniu do usuwania, umowa międzynarodowa może stanowić, że dane należy usunąć, jeżeli informacje były przetwarzane niezgodnie z prawem lub nie są już niezbędne do celów przetwarzania. Ponadto, w umowie międzynarodowej należy określić, że strony odpowiedzą na żądania osób, których dane dotyczą, w rozsądny i terminowy sposób. W umowie międzynarodowej można również wskazać, że strony mogą podjąć odpowiednie działania, w tym pobrać opłatę w rozsądnej wysokości w celu pokrycia kosztów administracyjnych, jeżeli żądania osoby, której dane dotyczą, są w sposób oczywisty nieuzasadnione lub nadmierne, w szczególności ze względu na swoją powtarzalność.

36. W umowie międzynarodowej należy również określić obowiązek przekazującego podmiotu publicznego udzielenia bez zbędnej zwłoki informacji osobie, której dane dotyczą – po przekazaniu dotyczących jej danych osobowych – na temat działań podjętych w związku z jej żądaniem na podstawie praw przewidzianych w tejże umowie międzynarodowej, a w tym celu należy określić w niej odpowiedni termin (np. jeden miesiąc). Ponadto, jeżeli strony nie podejmą działań w związku z żądaniem osoby, której dane dotyczą, wówczas taką osobę należy niezwłocznie – tj. w określonym odpowiednim terminie (np. w terminie miesiąca od otrzymania żądania) – poinformować o powodach niepodjęcia działań oraz o możliwości wniesienia skargi oraz skorzystania ze środków ochrony prawnej przed sądem.

37. W umowie międzynarodowej można również przewidzieć wyjątki od tych praw. Na przykład można określić wyjątki od prawa dostępu i prawa do usunięcia danych, takie jak te przewidziane w art. 15 ust. 4 i art. 17 ust. 3 RODO. Podobnie można przewidzieć wyjątki od praw indywidualnych w przypadku przetwarzania danych osobowych do celów badań naukowych lub historycznych, do celów

statystycznych lub do celów archiwalnych, o ile prawdopodobne jest, że takie prawa uniemożliwią lub poważnie utrudnią realizację celów takiego przetwarzania, oraz pod warunkiem zapewnienia odpowiednich zabezpieczeń (np. środków technicznych i organizacyjnych, w tym pseudonimizacji). Co więcej, umowa może stanowić, że strony mogą odmówić podjęcia działania w związku z żądaniem, które jest ewidentnie nieuzasadnione lub nadmierne.

2.4.3 Zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach

38. W stosownych przypadkach w odniesieniu do przedmiotowej umowy, umowy międzynarodowe zasadniczo powinny zawierać klauzulę stanowiącą, że otrzymujący podmiot publiczny nie podejmie decyzji wyłącznie na podstawie zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach, w tym profilowania, która to decyzja wywołuje wobec danej osoby, której dane dotyczą, skutki prawne lub w podobny sposób istotnie na nią wpływa. Jeżeli cel przekazywania danych wiąże się z możliwością podejmowania przez otrzymujący podmiot publiczny decyzji wyłącznie w oparciu o zautomatyzowane przetwarzanie w rozumieniu art. 22 RODO, powinno to nastąpić wyłącznie na określonych warunkach wskazanych w danej umowie międzynarodowej, na przykład konieczności uzyskania wyraźnej zgody osoby, której dane dotyczą. Jeżeli dana decyzja nie spełnia określonych warunków, osoba, której dane dotyczą, powinna mieć prawo do tego, by nie podlegać takiej decyzji. Jeżeli w danej umowie międzynarodowej dopuszcza się zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach, wówczas w każdym przypadku w takiej umowie należy zapewnić niezbędne zabezpieczenia, w tym prawo do uzyskania informacji o konkretnych powodach wydania decyzji i zasadach jej podjęcia, prawo do poprawienia nieprawidłowych informacji lub uzupełnienia niekompletnych informacji oraz prawo do zakwestionowania decyzji i prawo do uzyskania interwencji ludzkiej.

2.4.4 Prawo dochodzenia roszczeń

39. Chronione prawa osoby, której dane dotyczą, muszą być egzekwowalne i skuteczne. Z tego względu osoba, której dane dotyczą, musi mieć dostęp do środków zaskarżenia. Poniżej, w sekcji 2.7 i 3, przedstawiono różne przykładowe sposoby zapewnienia mechanizmów zaskarżenia.

2.4.5 Ograniczenia praw osób, których dane dotyczą

40. W umowie międzynarodowej należy również przewidzieć ograniczenia praw osób, których dane dotyczą. Ograniczenia te powinny być zgodnie z ograniczeniami przewidzianymi w art. 23 RODO. Takie ograniczenie musi być środkiem niezbędnym i proporcjonalnym w demokratycznym społeczeństwie służącym ważnym celom leżącym w interesie publicznym zgodnym z celami wymienionymi w art. 23 ust. 1 RODO, takimi jak prawa i wolności innych osób, bezpieczeństwo narodowe, obrona lub zapobieganie przestępczości, prowadzenie postępowań przygotowawczych, wykrywanie lub ściganie czynów zabronionych. Ograniczenie musi być określone w prawie lub, w przypadku organizacji międzynarodowych, w mających zastosowanie przepisach wewnętrznych/ramach regulacyjnych i obowiązywać wyłącznie przez okres, w którym istnieje powód jego stosowania.

2.5 Ograniczenia dotyczące dalszego przekazywania i udostępniania danych (w tym ujawniania i dostępu administracji rządowej)

41. W umowie międzynarodowej należy co do zasady wyraźnie wykluczyć dalsze przekazywanie danych przez otrzymujący podmiot publiczny lub otrzymującą organizację międzynarodową odbiorcom

niezwiązanym daną umową. W zależności od przedmiotu sprawy i konkretnych okoliczności strony mogą uznać, że dalsze przekazywanie danych jest konieczne. W takim przypadku, jeżeli spełniona jest zasada ograniczenia celu[20], umowa międzynarodowa powinna stanowić, że takie dalsze przekazywanie jest możliwe wyłącznie wówczas, gdy przekazujący podmiot publiczny udzielił uprzednio wyraźnej zgody, a otrzymujące strony trzecie zobowiązały się do przestrzegania zasad i zabezpieczeń w zakresie ochrony danych odpowiadających zasadom i zabezpieczeniom określonym w danej umowie międzynarodowej. Obejmuje to zobowiązanie do zapewnienia osobom, których dane dotyczą, tych samych praw i gwarancji w zakresie ochrony danych co w danej umowie międzynarodowej w celu dopilnowania, aby w przypadku dalszego przekazywania danych nie doszło do obniżenia stopnia ochrony.

42. Zasadniczo w odniesieniu do udostępniania danych osobowych w tym samym państwie zastosowanie powinny mieć te same zabezpieczenia co w przypadku dalszego przekazywania, tj. w umowie międzynarodowej należy wykluczyć takie dalsze udostępnianie, a odstępstwa zasadniczo należy dopuścić wyłącznie wówczas, gdy przekazujący podmiot publiczny udzielił uprzednio wyraźnej zgody, a otrzymujące strony trzecie zobowiązały się do przestrzegania zasad i zabezpieczeń w zakresie ochrony danych odpowiadających zasadom i zabezpieczeniom określonym w danej umowie międzynarodowej.

43. Zaleca się, aby przed zwróceniem się do przekazującego podmiotu publicznego z wnioskiem o udzielenie wyraźnej zgody otrzymujący podmiot publiczny lub otrzymująca organizacja międzynarodowa przedstawiły wystarczające informacje na temat rodzaju danych osobowych, które zamierzają przekazać/udostępnić, przyczyn i celów, ze względu na które uznały, że niezbędne jest przekazanie/udostępnienie danych osobowych oraz w przypadku dalszego przekazywania – informacje na temat państw lub organizacji, do których zamierzają dalej przekazać dane osobowe, co ma umożliwić ocenę przepisów danego państwa trzeciego lub, w przypadku organizacji międzynarodowych, mających zastosowanie przepisów wewnętrznych/ram regulacyjnych.

44. Jeżeli niezbędne jest dopuszczenie udostępnienia danych osobowych stronie trzeciej w państwie otrzymującego podmiotu publicznego lub innej organizacji międzynarodowej, w określonych okolicznościach można dopuścić udostępnienie danych za uprzednią wyraźną zgodą przekazującego podmiotu publicznego albo pod warunkiem, że otrzymująca strona trzecia w sposób wiążący zobowiązała się do przestrzegania zasad i gwarancji zawartych w danej umowie międzynarodowej.

45. Ponadto w umowie międzynarodowej można określić wyjątkowe okoliczności, w których dalsze udostępnianie jest możliwe bez uprzedniej zgody lub wyżej wspomnianych zobowiązań zgodnie z wyjątkami wymienionymi w art. 49 RODO, na przykład jeżeli takie szczególne udostępnienie jest niezbędne do ochrony żywotnych interesów osoby, których dane dotyczą, lub innych osób, lub też niezbędne do ustalenia, dochodzenia lub ochrony roszczeń. Tego rodzaju wyjątkowe okoliczności mogą występować również wówczas, gdy dalsze udostępnianie jest konieczne na mocy prawa strony otrzymującej na potrzeby bezpośrednio powiązanych postępowań przygotowawczych/sądowych.

46. W przypadkach wymienionych w powyższym punkcie w umowie międzynarodowej należy wyraźnie określić szczególne i wyjątkowe okoliczności, w których dopuszcza się tego rodzaju udostępnianie danych. Przed udostępnieniem danych otrzymujący podmiot publiczny lub otrzymująca organizacja międzynarodowa powinny być również zobowiązane do powiadomienia o tym fakcie przekazującego podmiotu publicznego i przedstawienia mu informacji na temat udostępnianych danych, otrzymującej strony trzeciej i podstawy prawnej udostępniania. Z kolei przekazujący podmiot publiczny powinien

[20] Zob. powyżej w sekcji 2.3.1.

prowadzić rejestr takich powiadomień od otrzymującego podmiotu publicznego lub otrzymującej organizacji międzynarodowej i przekazywać te informacje na żądanie swojemu organowi nadzorczemu. Jeżeli takie powiadomienie poprzedzające udostępnienie będzie stanowiło naruszenie obowiązków zachowania poufności przewidzianych w prawie, np. obowiązku zachowania poufności postępowania przygotowawczego, konkretne informacje należy przekazać najszybciej jak to możliwe po udostępnieniu. W takim przypadku przekazujący podmiot powinien regularnie otrzymywać ogólne informacje na temat rodzaju wniosków, jakie wpłynęły w określonym okresie, w tym informacje na temat kategorii danych, których dotyczyły wnioski, podmiotu składającego wniosek oraz podstawy prawnej ujawnienia danych.

47. We wszystkich powyższych scenariuszach umowa międzynarodowa powinna dopuszczać ujawnienie danych osobowych innym organom publicznym w państwie trzecim otrzymującego podmiotu publicznego wyłącznie w stopniu, który jest niezbędny i proporcjonalny w demokratycznym społeczeństwie do ochrony ważnych celów leżących w ogólnym interesie publicznym zgodnych z celami wymienionymi w art. 23 ust. 1 RODO oraz zgodnie z orzecznictwem TSUE. Aby przeprowadzić ocenę ewentualnego dostępu organów publicznych państwa trzeciego do celów nadzoru, przekazujący organ publiczny powinien uwzględnić elementy przypomniane w czterech niezbędnych gwarancjach europejskich[21]. Elementy te obejmują między innymi dostęp osób, których dane dotyczą, do skutecznych środków ochrony w państwie trzecim otrzymującego podmiotu publicznego w sytuacji, w której dostęp do ich danych osobowych mają organy publiczne[22]. Jeżeli dane przekazuje się organizacjom międzynarodowym, w każdym przypadku taki dostęp musi być zgodny z prawem międzynarodowym publicznym i bez uszczerbku w szczególności dla przywilejów i immunitetów danej organizacji międzynarodowej.

48. W zależności od konkretnego przypadku warto stosować wymóg dołączenia do umowy międzynarodowej załącznika zawierającego wykaz przepisów regulujących dalsze udostępnianie innym podmiotom publicznym, w tym do celów nadzoru w państwie przeznaczenia. O wszelkich zmianach tego załącznika należy powiadomić stronę przekazującą w określonym terminie.

2.6 Dane wrażliwe

49. Jeżeli w umowie międzynarodowej przewidziano przekazywanie danych wrażliwych w rozumieniu art. 9 ust. 1 RODO, należy uwzględnić dodatkowe zabezpieczenia dotyczące szczególnych rodzajów ryzyka, jakie otrzymujący podmiot publiczny lub otrzymująca organizacja międzynarodowa powinny wdrożyć. Takie zabezpieczenia mogą na przykład obejmować ograniczenia, takie jak ograniczenia dostępu, ograniczenia celów, do których informacje można przetwarzać, ograniczenia dalszego przekazywania itp. lub szczególne zabezpieczenia, np. dodatkowe środki bezpieczeństwa wymagające specjalistycznego przeszkolenia pracowników, którzy mogą uzyskać dostęp do informacji.

2.7 Mechanizmy zaskarżenia

50. Aby zagwarantować egzekwowalne i skuteczne prawa osób, których dane dotyczą, w umowie międzynarodowej należy zapewnić system, dzięki któremu osoby, których dane dotyczą, nadal mogą korzystać z mechanizmów zaskarżenia po przekazaniu dotyczących ich danych do państwa spoza EOG lub do organizacji międzynarodowej. Takie mechanizmy zaskarżenia muszą zapewnić możliwość dochodzenia roszczeń osobom fizycznym, które wskutek nieprzestrzegania przepisów wybranego instrumentu zostały poszkodowane, co oznacza, że w ramach tych mechanizmów należy zapewnić

[21] Zob. Zalecenia 02/2020 EROD dotyczące niezbędnych gwarancji europejskich dla środków nadzoru.
[22] Zob. Zalecenia 02/2020 EROD, gwarancja D, s. 13 i nast.

osobom, których dane osobowe zostały przekazane z EOG, możliwość składania skarg dotyczących tego rodzaju nieprzestrzegania przepisów oraz należy zagwarantować rozpatrzenie tych skarg. W szczególności osobie, której dane dotyczą, należy zapewnić skuteczny tryb składania skarg do podmiotów publicznych, które są stronami danej umowy międzynarodowej, i (bezpośrednio albo za pośrednictwem odpowiedniej strony) do niezależnego mechanizmu nadzoru. Ponadto zasadniczo powinien być dostępny środek ochrony prawnej przed sądem.

51. Po pierwsze, otrzymujący podmiot publiczny powinien zobowiązać się do wdrożenia mechanizmu skutecznego i terminowego rozpatrywania składanych przez osoby, których dane dotyczą, skarg w przedmiocie przestrzegania uzgodnionych zabezpieczeń w zakresie ochrony danych. Ponadto osoby, których dane dotyczą, muszą mieć możliwość uzyskania skutecznych administracyjnych środków zaskarżenia przed niezależnym organem nadzoru, w tym w miarę dostępności, niezależnym organem ochrony danych[23].

52. Po drugie, w umowie należy przewidzieć środek ochrony prawnej przed sądem, w tym możliwość uzyskania odszkodowania za szkody zarówno materialne, jak i niematerialne poniesione na skutek niezgodnego z prawem przetwarzania danych osobowych. Jeżeli nie można zapewnić skutecznych sądowych środków zaskarżenia, na przykład ze względu na ograniczenia w prawie krajowym lub szczególny status otrzymującego podmiotu publicznego, np. organizacji międzynarodowych, w umowie międzynarodowej należy określić alternatywne zabezpieczenia. W ramach takich alternatywnych zabezpieczeń osobom, których dane dotyczą, należy zapewnić gwarancje, które są merytorycznie równoważne gwarancjom wymaganym w art. 47 Karty Praw Podstawowych Unii Europejskiej („Karta UE")[24].

53. W tym przypadku w umowie międzynarodowej można ustanowić strukturę umożliwiającą osobie, której dane dotyczą, dochodzenie swoich praw na drodze pozasądowej, na przykład za pomocą quasi-sądowych, wiążących mechanizmów takich jak arbitraż lub alternatywnych metod rozwiązywania sporów takich jak mediacja, co zagwarantowałoby niezależną kontrolę i byłoby wiążące dla otrzymującego podmiotu publicznego[25]. Ponadto podmiot publiczny przekazujący dane osobowe może zobowiązać się do wypłaty odszkodowania za szkody wynikające z niezgodnego z prawem przetwarzania danych osobowych potwierdzonego w drodze niezależnej kontroli.
W wyjątkowych sytuacjach w umowie można wprowadzić inne, równie niezależne i skuteczne mechanizmy zaskarżenia, na przykład skuteczne mechanizmy zaskarżenia wdrażane przez organizacje międzynarodowe.

54. W odniesieniu do wszystkich wyżej wymienionych mechanizmów zaskarżenia w umowie międzynarodowej należy zobowiązać strony do wzajemnego informowania się o wyniku postępowania, w szczególności w przypadku odrzucenia lub braku rozstrzygnięcia skargi wniesionej przez osobę fizyczną.

55. Mechanizmowi zaskarżenia musi towarzyszyć możliwość zawieszenia lub zakończenia przekazywania danych osobowych na podstawie danej umowy międzynarodowej przez przekazujący podmiot publiczny, jeżeli stronom nie uda się rozstrzygnąć sporu na drodze polubownej, do czasu w którym podmiot ten uzna, że dana sprawa została w sposób zadowalający rozwiązana przez otrzymujący

[23] Zob. również sekcja 2.8 dotycząca mechanizmów nadzoru.
[24] Wyrok TSUE z 16 lipca 2020 r. w sprawie C-311/18, Data Protection Commissioner/Facebook Ireland Ltd i Maximillian Schrems („Schrems II"), pkt 96, 186 i nast.
[25] Wyrok TSUE z 6 października 2015 r. w sprawie C-362/14, Maximillian Schrems/Data Protection Commissioner („Schrems"), pkt 41 i 95; wyrok TSUE z 16 lipca 2020 r. w sprawie C-311/18, Data Protection Commissioner/Facebook Ireland Ltd i Maximillian Schrems („Schrems II"), pkt 186, 187, 189, 195 i nast.

podmiot publiczny. Jeżeli takie zawieszenie lub zakończenie przekazywania danych rzeczywiście ma miejsce, otrzymujący podmiot publiczny musi jednocześnie zobowiązać się do zwrotu lub usunięcia otrzymanych danych osobowych. O zawieszeniu lub zakończeniu przekazywania danych przekazujący podmiot publiczny musi powiadomić właściwy krajowy organ nadzorczy.

2.8 Mechanizmy nadzoru

56. W celu zapewnienia, aby wszystkie obowiązki ustanowione na mocy umowy międzynarodowej były przestrzegane, w umowie tej należy określić niezależny mechanizm nadzoru umożliwiający monitorowanie prawidłowego stosowania umowy oraz przypadków kolidowania z prawami przewidzianymi w tej umowie.

57. Po pierwsze, w umowie należy przewidzieć wewnętrzny mechanizm nadzoru zapewniający przestrzeganie jej postanowień. Każda strona umowy powinna przeprowadzać okresowe wewnętrzne kontrole obowiązujących procedur i skutecznego stosowania zabezpieczeń przewidzianych w umowie. W toku takich okresowych wewnętrznych kontroli należy również weryfikować wszelkie zmiany przepisów, które uniemożliwiłyby przestrzeganie przez strony zasad i zabezpieczeń w zakresie ochrony danych określonych w umowie międzynarodowej. Ponadto można określić, że strona umowy może zwrócić się do innej strony umowy z wnioskiem o przeprowadzenie takiego przeglądu. Umowa międzynarodowa musi zawierać nakaz udzielania odpowiedzi na zapytania drugiej strony dotyczące skutecznego wykonania zabezpieczeń przewidzianych w umowie. Każda strona przeprowadzająca przegląd powinna przedstawić wyniki kontroli drugiej stronie lub pozostałym stronom umowy. Najlepiej byłoby, gdyby informacje te były przekazywane również do niezależnego mechanizmu nadzoru, którym objęta jest dana umowa.

58. Ponadto umowa międzynarodowa musi stanowić, że strona ma obowiązek niezwłocznie poinformować drugą stronę, jeżeli z jakiegokolwiek powodu nie jest w stanie skutecznie wdrożyć zabezpieczeń przewidzianych w umowie. W takim przypadku umowa międzynarodowa musi przewidywać możliwość zawieszenia lub zakończenia przekazywania danych osobowych na podstawie tej umowy otrzymującemu podmiotowi publicznemu przez przekazujący podmiot publiczny do czasu, w którym otrzymujący podmiot publiczny poinformuje przekazujący podmiot publiczny, że ponownie jest w stanie działać z poszanowaniem przewidzianych zabezpieczeń. O zmianie sytuacji, a także o zawieszeniu przekazywania danych lub rozwiązaniu umowy podmiot przekazujący musi powiadomić właściwy krajowy organ nadzorczy.

59. Po drugie, w umowie należy przewidzieć niezależny mechanizm nadzoru odpowiadający za zapewnienie, aby strony przestrzegały postanowień umowy. Wymóg ten wynika bezpośrednio z Karty Praw Podstawowych UE[26] i Europejskiej Konwencji Praw Człowieka (EKPC)[27] zgodnie z orzecznictwem Europejskiego Trybunału Praw Człowieka i na warunkach określonych w prawie pierwotnym[28], a także powiązanym orzecznictwie.

[26] Art. 7, 8 i 47 Karty Praw Podstawowych UE.
[27] Art. 8 EKPC.
[28] Art. 6 Traktatu z Lizbony.
1. Unia uznaje prawa, wolności i zasady określone w Karcie praw podstawowych Unii Europejskiej z 7 grudnia 2000 roku, w brzmieniu dostosowanym 12 grudnia 2007 roku w Strasburgu, która ma taką samą moc prawną jak Traktaty.
Postanowienia Karty w żaden sposób nie rozszerzają kompetencji Unii określonych w Traktatach.
Prawa, wolności i zasady zawarte w Karcie są interpretowane zgodnie z postanowieniami ogólnymi określonymi w tytule VII Karty regulującymi jej interpretację i stosowanie oraz z należytym uwzględnieniem wyjaśnień, o których mowa w Karcie, które określają źródła tych postanowień.
2. Unia przystępuje do europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności. Przystąpienie do Konwencji nie ma wpływu na kompetencje Unii określone w Traktatach.
3. Prawa podstawowe, zagwarantowane w europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności oraz wynikające z tradycji konstytucyjnych wspólnych Państwom Członkowskim, stanowią część prawa Unii jako zasady ogólne prawa.

60. Od 2015 r.[29] Trybunał Sprawiedliwości Unii Europejskiej kilkukrotnie potwierdził konieczność obowiązywania niezależnego mechanizmu zaskarżenia i nadzoru[30]. Podobnie Europejski Trybunał Praw Człowieka wielokrotnie podkreślał w swoich wyrokach, że każdy przypadek kolidowania z prawem do poszanowania życia prywatnego określonym w art. 8 EKPC musi podlegać skutecznemu, niezależnemu i bezstronnemu systemowi nadzoru[31].

61. W umowie można na przykład określić, że nadzór sprawuje właściwy organ nadzorczy, jeżeli taki organ funkcjonuje w państwie podmiotu publicznego otrzymującego dane osobowe z EOG, nawet jeżeli w RODO nie wskazano, że właściwy organ nadzorczy musi pełnić rolę zewnętrznego organu nadzoru. Ponadto umowa może obejmować dobrowolne zobowiązanie strony otrzymującej do współpracy z organami nadzorczymi w EOG.

62. W przypadku braku organu nadzorczego odpowiedzialnego w szczególności za nadzór nad przepisami prawa w dziedzinie ochrony danych w państwie trzecim lub w organizacji międzynarodowej potrzebę zapewnienia niezależnych, skutecznych i bezstronnych mechanizmów nadzoru należy zaspokoić w inny sposób. Rodzaj stosowanego niezależnego mechanizmu nadzoru może zależeć od konkretnej sytuacji.

63. Umowa mogłaby na przykład dotyczyć istniejących w państwie trzecim organów nadzoru innych niż organ nadzorczy ds. ochrony danych. Ponadto, jeżeli ze strukturalnego lub instytucjonalnego punktu widzenia nie można zapewnić niezależnego nadzoru zewnętrznego, np. ze względu na przywileje i immunitety niektórych organizacji międzynarodowych, nadzór można zagwarantować za pomocą funkcjonalnie autonomicznych mechanizmów. Mechanizm taki musi obejmować organ, który choć sam nie jest organem zewnętrznym, wypełnia swoje zadania w sposób niezależny, tj. nie wykonuje poleceń, dysponuje wystarczającymi zasobami ludzkimi, technicznymi i finansowymi itp. Decyzje organu nadzoru są wiążące dla strony otrzymującej.

2.9 Klauzula regulująca rozwiązanie umowy

64. W umowie międzynarodowej należy przewidzieć, że wszelkie dane osobowe przekazane z EOG na podstawie umowy międzynarodowej przed jej faktycznym rozwiązaniem będą nadal przetwarzane zgodnie z postanowieniami umowy międzynarodowej.

[29] Wyrok TSUE z 6 października 2015 r. w sprawie C-362/14, Maximillian Schrems/Data Protection Commissioner („Schrems"), pkt 41 i 95.
[30] Opinia 1/15 TSUE z 27 lipca 2017 r. dotycząca umowy między Kanadą a Unią Europejską o przekazywaniu i przetwarzaniu danych dotyczących przelotu pasażera, 26 lipca 2017 r., pkt 228 i nast.; TSUE, 30 kwietnia 2019 r., opinia 1/17 dotycząca Kompleksowej umowy gospodarczo-handlowej między Kanadą a Unią Europejską, pkt 190 i nast.
[31] Orzeczenie Europejskiego Trybunału Praw Człowieka z 6 września 1978 r., Klass/Niemcy, pkt 55 i 56. Wymóg wynikający z orzeczenia Europejskiego Trybunału Praw Człowieka dotyczy również każdego przypadku kolidowania z art. 7 i 8 Karty UE, gdyż – zgodnie z art. 52 ust. 3 Karty UE – znaczenie i zakres tych praw podstawowych są takie same jak praw przyznanych w art. 8 EKPC.

3 SZCZEGÓŁOWE INFORMACJE NA TEMAT ART. 46 RODO

3.1 Szczegółowe informacje na temat prawnie wiążących i egzekwowalnych instrumentów – art. 46 ust. 2 lit. a) RODO

65. Zgodnie z art. 46 ust. 2 lit. a) RODO podmioty publiczne z EOG mogą przekazywać dane osobowe do państwa trzeciego lub organizacji międzynarodowej w oparciu o zawarte instrumenty, bez konieczności uzyskania uprzedniego zezwolenia ze strony organu nadzorczego. Takie instrumenty muszą być prawnie wiążące i egzekwowalne. Zgodnie z tym przepisem można zatem stosować traktaty międzynarodowe, traktaty publicznoprawne lub administracyjne umowy samowykonalne.

66. Zgodnie z wymogami RODO każdy prawnie wiążący i egzekwowalny instrument powinien obejmować podstawowy zbiór zasad ochrony danych i praw osób, których dane dotyczą.

67. Strony mają obowiązek stosowania wystarczających zabezpieczeń w zakresie ochrony danych przy przekazywaniu danych osobowych. W umowie należy zatem również określić sposób, w jaki otrzymujący podmiot publiczny będzie stosował zbiór podstawowych zasad ochrony danych i praw osób, których dane dotyczą, do wszystkich przekazywanych danych osobowych, aby zgodnie z RODO zagwarantować odpowiedni stopień ochrony osób fizycznych.

68. Jeżeli nie ma możliwości zapewnienia skutecznych sądowych środków zaskarżenia za pomocą prawnie wiążących i egzekwowalnych instrumentów, w związku z czym konieczne jest uzgodnienie alternatywnych mechanizmów zaskarżenia, podmioty publiczne z EOG powinny zasięgnąć opinii właściwego organu nadzorczego przed zawarciem takich instrumentów.

69. Nawet jeśli forma instrumentu nie jest rozstrzygająca, ale jest on prawnie wiążący i egzekwowalny, według EROD najlepszym rozwiązaniem byłoby włączenie szczegółowych klauzul ochrony danych bezpośrednio do instrumentu. Jeżeli jednak ze względu na szczególne okoliczności rozwiązania tego nie można zastosować, EROD zdecydowanie zaleca uwzględnienie co najmniej ogólnej klauzuli określającej zasady ochrony danych bezpośrednio w treści instrumentu oraz umieszczenie bardziej szczegółowych przepisów i zabezpieczeń w załączniku do tego instrumentu.

3.2 Szczegółowe informacje na temat uzgodnień administracyjnych – art. 46 ust. 3 lit. b) RODO

70. W art. 46 ust. 3 lit. b) RODO przewidziano alternatywne instrumenty w postaci uzgodnień administracyjnych, np. protokołu ustaleń, które służą zapewnieniu ochrony poprzez zobowiązania podjęte przez obie strony w celu realizacji ich wspólnych uzgodnień.

71. W tym kontekście w art. 46 ust. 1 i motywie 108 RODO określono, że uzgodnienia te muszą uwzględniać zapewnienie egzekwowalnych praw osób, których dane dotyczą, i skutecznych środków ochrony prawnej. W przypadku gdy w uzgodnieniach administracyjnych, które nie są prawnie wiążące, przewidziano zabezpieczenia, należy uzyskać zezwolenie właściwego organu nadzorczego.

72. Należy dokładnie ocenić, czy powinno się skorzystać z niewiążących prawnie uzgodnień administracyjnych w celu zapewnienia zabezpieczeń w sektorze publicznym, biorąc pod uwagę cel przetwarzania i charakter danych. Jeżeli prawo krajowe państwa trzeciego lub przepisy wewnętrzne/ramy regulacyjne organizacji międzynarodowej nie przewidują praw ochrony danych osobowych i środków zaskarżenia dla osób fizycznych z EOG, należy w pierwszej kolejności zawrzeć

prawnie wiążącą umowę. Niezależnie od przyjętego instrumentu obowiązujące środki muszą być skuteczne, aby zapewnić odpowiednie wdrożenie, egzekwowanie i nadzór.

73. W ramach uzgodnień administracyjnych należy przedsięwziąć kroki w celu zapewnienia skutecznych praw indywidualnych, środków zaskarżenia i nadzoru. W szczególności, aby zapewnić skuteczne i egzekwowalne prawa, niewiążący instrument powinien obejmować zapewnienia ze strony podmiotu publicznego otrzymującego dane osobowe z EOG, że w jego prawie krajowym w pełni uwzględniono prawa indywidualne, z których osoby fizyczne z EOG mogą korzystać na tych samych warunkach co obywatele i rezydenci danego państwa trzeciego. To samo dotyczy sytuacji, w której osoby z EOG mają dostęp do administracyjnych i sądowych środków zaskarżenia w granicach krajowych ram prawnych otrzymującego podmiotu publicznego. Podobnie, organizacje międzynarodowe powinny przedstawić zapewnienia dotyczące praw indywidualnych wynikających z ich przepisów wewnętrznych, jak również dotyczące dostępnych mechanizmów zaskarżenia.

74. Jeżeli tak nie jest, prawa indywidualne należy zagwarantować w drodze konkretnych zobowiązań stron w połączeniu z mechanizmami proceduralnymi, aby zapewnić ich skuteczność i możliwość zaskarżenia po stronie osób fizycznych. Te konkretne zobowiązania i mechanizmy proceduralne muszą umożliwiać w praktyce zapewnienie zgodności ze stopniem ochrony merytorycznie równoważnym temu gwarantowanemu w UE na podstawie RODO.
Takie mechanizmy proceduralne mogą na przykład obejmować zobowiązania stron do wzajemnego informowania się o żądaniach osób fizycznych z EOG oraz do terminowego rozstrzygania sporów lub roszczeń.

75. Ponadto w przypadku gdy strony samodzielnie nie mogą rozwiązać takich sporów lub roszczeń w sposób polubowny, osobie fizycznej należy – za pomocą alternatywnych mechanizmów – zapewnić możliwość uzyskania niezależnych i skutecznych środków zaskarżenia, np. poprzez umożliwienie jej skorzystania z alternatywnego mechanizmu rozstrzygania sporów, takiego jak arbitraż lub mediacja. Taki alternatywny mechanizm rozstrzygania sporów musi mieć charakter wiążący[32].

76. W zależności od konkretnego przypadku w umowie administracyjnej należy przewidzieć połączenie wszystkich lub niektórych ze wspomnianych środków w celu zapewnienia skutecznych środków zaskarżenia. Dopuszczalne jest także zastosowanie innych środków nieuwzględnionych w tych wytycznych, o ile służą one zapewnieniu niezależnych i skutecznych środków zaskarżenia.

77. Każde uzgodnienie administracyjne opracowane zgodnie z art. 46 ust. 3 lit. b) RODO zostanie indywidualnie sprawdzone przez właściwy organ nadzorczy, a następnie, w stosownych przypadkach, zostanie poddane odpowiedniej procedurze EROD. Właściwy organ nadzorczy sprawdzi te uzgodnienia w oparciu o ogólne zalecenia określone w niniejszych wytycznych, ale w poszczególnych przypadkach może także wnieść o zapewnienie większych gwarancji.

[32] Wyrok TSUE z 16 lipca 2020 r., w sprawie C-311/18, Data Protection Commissioner/Facebook Ireland Ltd i Maximillian Schrems („Schrems II"), pkt 189, 196 i nast.

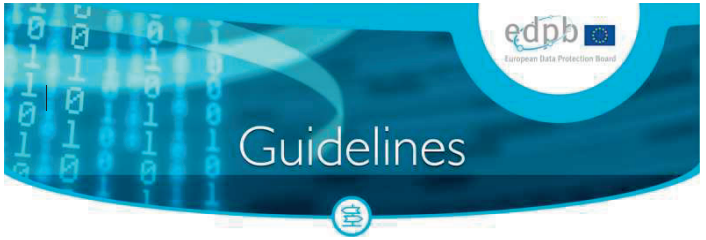
4 PYTANIA DOTYCZĄCE KWESTII PROCEDURALNYCH

78. Uzgodnienia administracyjne na podstawie art. 46 ust. 3 lit. b) RODO będą sprawdzane indywidualnie ze względu na wymogi dotyczące uzyskania zezwolenia od właściwego organu nadzorczego, który zgodnie z art. 46 ust. 4 RODO stosuje mechanizm spójności opisany w art. 64 ust. 2 RODO. EROD zaleca również, aby przy włączaniu alternatywnych mechanizmów zaskarżenia do wiążących i egzekwowalnych instrumentów zgodnie z art. 46 ust. 2 lit. a) RODO zasięgnąć porady właściwego organu nadzorczego. EROD zdecydowanie radzi, aby konsultować się z właściwym organem nadzorczym na wczesnym etapie.

W imieniu Europejskiej Rady Ochrony Danych

Przewodnicząca

(Andrea Jelinek)



Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications

Version 2.0

Adopted on 9 March 2021

Version history

Version 2.0	9 March 2021	Adoption of the Guidelines after public consultation
Version 1.0	28 January 2020	Adoption of the Guidelines for public consultation

Table of contents

1 INTRODUCTION 4
1.1 Related works 5
1.2 Applicable law 6
1.3 Scope 8
1.4 Definitions 11
1.5 Privacy and data protection risks 13
2 GENERAL RECOMMENDATIONS 15
2.1 Categories of data 15
2.2 Purposes 17
2.3 Relevance and data minimisation 17
2.4 Data protection by design and by default 18
2.5 Information 21
2.6 Rights of the data subject 23
2.7 Security 23
2.8 Transmitting personal data to third parties 24
2.9 Transfer of personal data outside the EU/EEA 25
2.10 Use of in-vehicle Wi-Fi technologies 26
3 CASE STUDIES 26
3.1 Provision of a service by a third party 26
3.2 eCall 30
3.3 Accidentology studies 33
3.4 Tackle auto theft 35

The European Data Protection Board

Having regard to Article 70 (1) (e) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, (hereinafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018[1],

Having regard to Article 12 and Article 22 of its Rules of Procedure,

HAS ADOPTED THE FOLLOWING GUIDELINES

1 INTRODUCTION

1. Symbol of the 20th century economy, the automobile is one of the mass consumer products that has impacted society as a whole. Commonly associated with the notion of freedom, cars are often considered as more than just a means of transportation. Indeed, they represent a private area in which people can enjoy a form of autonomy of decision, without encountering any external interferences. Today, as connected vehicles move into the mainstream, such a vision no longer corresponds to the reality. In-vehicle connectivity is rapidly expanding from luxury models and premium brands to high-volume midmarket models, and vehicles are becoming massive data hubs. Not only vehicles, but drivers and passengers are also becoming more and more connected. As a matter of fact, many models launched over the past few years on the market integrate sensors and connected on-board equipment, which may collect and record, among other things, the engine performance, the driving habits, the locations visited, and potentially even the driver's eye movements, his or her pulse, or biometric data for the purpose of uniquely identifying a natural person.[2]

2. Such data processing is taking place in a complex ecosystem, which is not limited to the traditional players of the automotive industry, but is also shaped by the emergence of new players belonging to the digital economy. These new players may offer infotainment services such as online music, road condition and traffic information, or provide driving assistance systems and services, such as autopilot software, vehicle condition updates, usage-based insurance or dynamic mapping. Moreover, since vehicles are connected via electronic communication networks, road infrastructure managers and telecommunications operators involved in this process also play an important role with respect to the potential processing operations applied to the drivers' and passengers' personal data.

3. In addition, connected vehicles are generating increasing amounts of data, most of which can be considered personal data since they will relate to drivers or passengers. Even if the

[1] References to "Member States" made throughout this document should be understood as references to "EEA Member States".
[2] Infographic "Data and the connected car" by the Future of Privacy Forum; https://fpf.org/wp-content/uploads/2017/06/2017_0627-FPF-Connected-Car-Infographic-Version-1.0.pdf

data collected by a connected car are not directly linked to a name, but to technical aspects and features of the vehicle, it will concern the driver or the passengers of the car. As an illustration, data relating to the driving style or the distance covered, data relating to the wear and tear on vehicle parts, location data or data collected by cameras may concern driver behaviour as well as information about other people who could be inside or data subjects that pass by. Such technical data are produced by a natural person, and permit his/her direct or indirect identification, by the data controller or by another person. The vehicle can be considered as a terminal that can be used by different users. Therefore, as for a personal computer, this potential plurality of users does not affect the personal nature of the data.

4. In 2016, the Fédération Internationale de l'Automobile (FIA) ran a campaign across Europe called "My Car My Data" to get a sentiment on what Europeans think about connected cars.[3] While it showed the high interest of drivers for connectivity, it also highlighted the vigilance that must be exercised with regard to the use of the data produced by vehicles as well as the importance of complying with personal data protection legislation. Thus, the challenge is, for each stakeholder, to incorporate the "protection of personal data" dimension from the product design phase, and to ensure that car users enjoy transparency and control in relation to their data in accordance with recital 78 GDPR. Such an approach helps to strengthen user confidence, and thus the long-term development of those technologies.

1.1 Related works

5. Connected vehicles have become a substantial subject for regulators over the last decade, with a major increase in the last couple of years. Various works have thus been published at the national and international levels concerning the security and privacy of connected vehicles. Those regulations and initiatives aim at complementing the existing data protection and privacy frameworks with sector specific rules or providing guidance to professionals.

1.1.1 European-level and international initiatives

6. Since 31 March 2018, a 112-based eCall in-vehicle system is mandatory on all new types of M1 and N1 vehicles (passenger cars and light duty vehicles).[4,5] In 2006, the Article 29 Working Party had already adopted a working document on data protection and privacy implications in eCall initiative.[6] In addition, as previously discussed, the Article 29 Working Party also adopted an opinion in October 2017 regarding the processing of personal data in the context of Cooperative Intelligent Transport Systems (C-ITS).

7. In January 2017, the European Union Agency for Network and Information Security (ENISA) published a study focused on cyber security and resilience of smart cars listing the sensitive assets as well as the corresponding threats, risks, mitigation factors and possible security measures to implement.[7] In September 2017, the International Conference of Data Protection and Privacy Commissioners (ICDPPC) adopted a resolution on connected vehicles.[8] Finally, in April 2018, the International Working Group on Data Protection in Telecommunications (IWGDPT), also adopted a working paper on connected vehicles.[9]

1.1.2 National initiatives of European Data Protection Board (EDPB) members

8. In January 2016, the Conference of the German Federal and State Data Protection Authorities and the German Association of the Automotive Industry (VDA) published a common declaration on the principles of data protection in connected and not-connected vehicles.[10] In August 2017, the UK Centre for Connected and Autonomous Vehicles (CCAV) released a guide stating principles of cyber security for connected and automated vehicles in order to raise awareness on the matter within the automotive sector.[11] In October 2017, the French data protection authority, the Commission Nationale de l'Informatique et des Libertés (CNIL), released a compliance package for connected cars in order to provide assistance to stakeholders on how to integrate data protection by design and by default, enabling data subjects to have effective control over their data.[12]

1.2 Applicable law

9. The relevant EU legal framework is the GDPR. It applies in any case where data processing in the context of connected vehicles involves processing personal data of individuals.

10. Additionally to the GDPR, directive 2002/58/EC as revised by 2009/136/EC (hereinafter – "ePrivacy directive"), **sets a specific standard for all actors that wish to store or access information stored in the terminal equipment of a subscriber or user in the European Economic Area (EEA).**

11. Indeed, if most of the ePrivacy directive provisions (art. 6, art. 9, etc.) only apply to providers of publicly available electronic communication services and providers of public communication networks, art. 5(3) ePrivacy directive is a general provision. It does not only apply to electronic communication services but also to every entity, private or public, that places on or reads information from a terminal equipment without regard to the nature of the data being stored or accessed.

[3] Campaign "My Car My Data"; http://www.mycarmydata.eu/.
[4] The interoperable EU-wide eCall; https://ec.europa.eu/transport/themes/its/road/action_plan/ecall_en.
[5] Decision No 585/2014/EU of the European Parliament and of the Council of 15 May 2014 on the deployment of the interoperable EU-wide eCall service Text with EEA relevance; https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014D0585.
[6] Working document on data protection and privacy implications in eCall initiative; http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp125_en.pdf.
[7] Cyber security and resilience of smart cars; https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars.
[8] Resolution on data protection in automated and connected vehicles; https://edps.europa.eu/sites/edp/files/publication/resolution-on-data-protection-in-automated-and-connected-vehicles_en_1.pdf.
[9] Working paper on connected vehicles; https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/working-paper/.
[10] Data protection aspects of using connected and non-connected vehicles; https://www.lda.bayern.de/media/dsk_joint_statement_vda.pdf.
[11] Principles of cyber security for connected and automated vehicles; https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles.
[12] Compliance package for a responsible use of data in connected cars; https://www.cnil.fr/en/connected-vehicles-compliance-package-responsible-use-data.

12. Regarding the notion of "*terminal equipment*", the definition is given by directive 2008/63/CE[13]. Art. 1 (a) defines the terminal equipment as an *"equipment directly or indirectly connected to the interface of a public telecommunications network to send, process or receive information; in either case (direct or indirect), the connection may be made by wire, optical fibre or electromagnetically; a connection is indirect if equipment is placed between the terminal and the interface of the network; (b) satellite earth station equipment"*.

13. As a result, provided that the aforementioned criteria are met, the connected vehicle and device connected to it should be considered as a *"terminal equipment"* (just like a computer, a smartphone or a smart TV) and provisions of art. 5(3) ePrivacy directive apply where relevant.

14. As outlined by the EDPB in its opinion 5/2019 on the interplay between the ePrivacy directive and the GDPR,[14] art. 5(3) ePrivacy directive provides that, as a rule, and subject to the exceptions to that rule mentioned in paragraph 17 below, prior consent is required for the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user. To the extent that the information stored in the end-user's device constitutes personal data, art. 5(3) ePrivacy directive shall take precedence over art. 6 GDPR with regards to the activity of storing or gaining access to this information.[15] Any processing operations of personal data following the aforementioned processing operations, including processing personal data obtained by accessing information in the terminal equipment, must have a legal basis under art. 6 GDPR in order to be lawful.[16]

15. Since the controller, when seeking consent for the storing or gaining of access to information pursuant to art. 5(3) ePrivacy directive, will have to inform the data subject about all the purposes of the processing – including any processing following the aforementioned operations (meaning the "subsequent processing") – consent under art. 6 GDPR will generally be the most adequate legal basis to cover the processing of personal data following such operations (as far as the purpose of the following processing is comprehended by the data subject´s consent, see paragraphs 53-54 below). Hence, consent will likely constitute the legal basis both for the storing and gaining of access to information already stored and the subsequent processing of personal data[17]. Indeed, when assessing compliance with art. 6 GDPR, one should take into account that the processing as a whole involves specific activities for which the EU legislature has sought to provide additional protection.[18] Moreover, controllers must take into account the impact on data subjects' rights when identifying the appropriate lawful basis in order to respect the principle of fairness.[19] The bottom line is that art. 6 GDPR cannot be relied upon by controllers in order to lower the additional protection provided by art. 5(3) ePrivacy directive.

16. The EDPB recalls that the notion of consent in the ePrivacy directive remains the notion of consent in the GDPR and must meet all the requirements of the consent as provided by art. 4(11) and 7 GDPR.

17. However, while consent is the principle, art. 5(3) ePrivacy directive allows the storing of information or the gaining of access to information that is already stored in the terminal equipment to be exempted from the requirement of informed consent, if it satisfies one of the following criteria:

    - **Exemption 1:** for the sole purpose of carrying out the transmission of a communication over an electronic communications network;
    - **Exemption 2:** when it is strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.

18. In such cases, the processing of personal data including personal data obtained by accessing information in the terminal equipment is based on one of the legal bases as provided by art. 6 GDPR. For example, consent is not needed when data processing is necessary to provide GPS navigation services requested by the data subject when such services can be qualified as information society services.

1.3 Scope

19. The EDPB would like to point out that these guidelines are intended to facilitate compliance of the processing of personal data carried out by a wide range of stakeholders working in this environment. However, they are not intended to cover all use cases possible in this context or to provide guidance for every possible specific situation.

20. The scope of this document focuses in particular on the personal data processing in relation to the non-professional use of connected vehicles by data subjects: e.g., drivers, passengers, vehicle owners, other road users, etc. More specifically, it deals with the personal data: (i) processed inside the vehicle, (ii) exchanged between the vehicle and personal devices connected to it (e.g., the user's smartphone) or (iii) collected locally in the vehicle and exported to external entities (e.g., vehicle manufacturers, infrastructure managers, insurance companies, car repairers) for further processing.

21. The connected vehicle definition has to be understood as a broad concept in this document. It can be defined as a vehicle equipped with many electronic control units (ECU) that are linked together via an in-vehicle network as well as connectivity facilities allowing it to share information with other devices both inside and outside the vehicle. As such, data can be exchanged between the vehicle and personal devices connected to it, for instance allowing the mirroring of mobile applications to the car's in-dash information and entertainment unit. Also, the development of standalone mobile applications, meaning independent of the vehicle (for example, relying on the sole use of the smart phone) to assist drivers is included

[13] Commission Directive 2008/63/EC of 20 June 2008 on competition in the markets in telecommunications terminal equipment (Codified version) (Text with EEA relevance); https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32008L0063.
[14] European Data Protection Board, Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities, adopted on 12 March 2019 (hereinafter - "Opinion 5/2019"), paragraph 40.
[15] Ibid, paragraph 40.
[16] Ibid, paragraph 41.
[17] Consent required by art. 5(3) of the "ePrivacy" directive and consent needed as a legal basis for the processing of data (art. 6 GDPR) for the same specific purpose can be collected at the same time (for example, by checking a box clearly indicating what the data subject is consenting to).
[18] Opinion 5/2019, paragraph 41.
[19] European Data Protection Board, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0, 8 October 2019, paragraph 1.

in the scope of this document since they contribute to the vehicle's connectivity capacities even though they may not effectively rely on the transmission of data with the vehicle *per se*. Applications for connected vehicles are multiple and diverse and can include[20]:

22. *Mobility management:* functions that allow drivers to reach a destination quickly, and in a cost-efficient manner, by providing timely information about GPS navigation, potentially dangerous environmental conditions (e.g., icy roads), traffic congestion or road construction work, parking lot or garage assistance, optimised fuel consumption or road pricing.

23. *Vehicle management:* functions that are supposed to aid drivers in reducing operating costs and improving ease of use, such as notification of vehicle condition and service reminders, transfer of usage data (e.g., for vehicle repair services), customised "*Pay As/How You Drive*" insurances, remote operations (e.g., heating system) or profile configurations (e.g., seat position).

24. *Road safety:* functions that warn the driver of external hazards and internal responses, such as collision protection, hazard warnings, lane departure warnings, driver drowsiness detection, emergency call (eCall) or crash investigation "black-boxes" (event data recorder).

25. *Entertainment:* functions providing information to and involving the entertainment of the driver and passengers, such as smart phone interfaces (hands free phone calls, voice generated text messages), WLAN hot spots, music, video, Internet, social media, mobile office or "smart home" services.

26. *Driver assistance:* functions involving partially or fully automated driving, such as operational assistance or autopilot in heavy traffic, in parking, or on highways,

27. *Well-being:* functions monitoring the driver's comfort, ability and fitness to drive such as fatigue detection or medical assistance.

28. Hence, vehicles can be natively connected or not and personal data can be collected through several means, including: (i) vehicle sensors, (ii) telematics boxes or (iii) mobile applications (e.g. accessed from a device belonging to a driver). In order to fall within the scope of this document, mobile applications need to be related to the environment of driving. For example, GPS navigation applications are in-scope. Applications whose functionalities only suggest places of interest (restaurants, historic monument, etc.) to drivers fall, however, outside the scope of these guidelines.

29. Much of the data that is generated by a connected vehicle relate to a natural person that is identified or identifiable and thus constitute personal data. For instance, data include directly identifiable data (e.g., the driver's complete identity), as well as indirectly identifiable data such as the details of journeys made, the vehicle usage data (e.g., data relating to driving style or the distance covered), or the vehicle's technical data (e.g., data relating to the wear and tear on vehicle parts), which, by cross-referencing with other files and especially the vehicle identification number (VIN), can be related to a natural person. Personal data in connected vehicles can also include metadata, such as vehicle maintenance status. In other words, any data that can be associated with a natural person therefore fall into the scope of this document.

[20] PwC Strategy 2014. "In the fast lane. The bright future of connected cars": https://www.strategyand.pwc.com/media/file/Strategyand_In-the-Fast-Lane.pdf.

30. The connected vehicle ecosystem covers a wide spectrum of stakeholders. This ecosystem more precisely includes traditional actors of the automotive industry as well as emerging players from the digital industry. Hence, these guidelines are directed towards vehicle manufacturers, equipment manufacturers and automotive suppliers, car repairers, automobile dealerships, vehicle service providers, fleet managers, motor insurance companies, entertainment providers, telecommunication operators, road infrastructure managers and public authorities as well as data subjects. The EDPB underlines that the categories of data subjects will differ from one service to another (e.g., drivers, owners, passengers, etc.). This is a non-exhaustive list as the ecosystem entails a wide variety of services, including services for which a direct authentication or identification is needed and services for which this is not needed.

31. Some data processing performed by natural persons within the vehicle fall within "*the course of a purely personal or household activity*" and are consequently out of the scope of the GDPR[21]. In particular, this concerns the use of personal data within the vehicles by the sole data subjects who provided such data into the vehicle's dashboard. However, the EDPB recalls that according to its recital 18 the GDPR "*applies to controllers or processors which provide the means for processing personal data for such personal or household activities*".

1.3.1 Out of scope of this document

32. Employers providing company cars to members of their staff might want to monitor their employee's actions (e.g., in order to ensure the safety of the employee, goods or vehicles, to allocate resources, to track and bill a service or to check working time). Data processing carried out by employers in this context raises specific considerations to the employment context, which might be regulated by labour laws at the national level that cannot be detailed in these guidelines[22].

33. While the data processing in the context of commercial vehicles used for professional purposes (such as public transport) and shared transport and MaaS solution may raise specific considerations which fall out of the scope of these general guidelines, many of the principles and recommendations set out here will also be applicable to those types of processing.

34. Connected vehicles being radio-enabled systems, they are subject to passive tracking such as Wi-Fi or Bluetooth tracking. In that sense they do not differ from other connected devices and fall in the scope of the ePrivacy directive which is currently being revised. This therefore excludes also large-scale tracking of Wi-Fi equipped vehicles[23] by a dense network of bystanders who use common smartphone location services. These routinely report all visible Wi-Fi networks to central servers. Since built-in Wi-Fi can be considered a secondary vehicle

[21] See GDPR, Article 2(2)(c).
[22] The Article 29 Working Party elaborated on this in its WP 249 Opinion 2/2017 on data processing at work; https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169.
[23] See for details: https://www.datenschutzzentrum.de/artikel/1269-Location-Services-can-Systematically-Track-Vehicles-with-WiFi-Access-Points-at-Large-Scale.html.

identifier[24], this risks a systematic ongoing collection of complete vehicle movement profiles.

35. Vehicles are increasingly equipped with image recording devices (e.g., car parking camera systems or dashcams). Since this deals with the issue of filming public places, which requires an assessment of the relevant legislative framework which is specific to each Member State, this data processing is out of the scope of these guidelines.

36. The processing of data enabling Cooperative Intelligent Transport Systems (C-ITS) – as defined in the directive 2010/40/EU[25] has been dealt with in a specific opinion by the Article 29 Working Party[26]. While the definition of the C-ITS concept in the directive does not bear any technical specifications, the Article 29 Working Party focuses in its opinion on short-range communications, i.e. that do not involve the intervention of a network operator. More specifically, it provides analysis for specific use cases built for initial deployment and committed to assess at a later stage the new issues that will be undoubtedly raised when higher level of automation will be implemented. Since the data protection implications in the context of C-ITS are very specific (unprecedented amounts of location data, continuous broadcasting of personal data, exchange of data between vehicles and other road infrastructural facilities, etc.) and that it is still being discussed at the European level, the processing of personal data in that context is not covered by these guidelines.

37. Finally, this document does not aim to address all possible issues and questions raised by connected vehicles and can therefore not be considered as exhaustive.

1.4 Definitions

38. The **processing** of personal data encompasses any operation that involves personal data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction, etc.[27]

39. The **data subject** is the natural person to whom the data covered by the processing relate. In the context of connected vehicles, it can, in particular, be the driver (main or occasional), the passenger, or the owner of the vehicle.[28]

40. The **data controller** is the person who determines the purposes and means of processing that take place in connected vehicles.[29] Data controllers can include service providers that process vehicle data to send the driver traffic-information, eco-driving messages or alerts

[24] Markus Ullmann, Tobias Franz, and Gerd Nolden, Vehicle Identification Based on Secondary Vehicle Identifier -- Analysis, and Measurements, in Proceedings, VEHICULAR 2017, The Sixth International Conference on Advances in Vehicular Systems, Technologies and Applications, Nice, France, July 23 to 27, 2017, p. 32-37.
[25] Directive 2010/40/EU of 7 July 2020 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport; https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32010L0040.
[26] Article 29 Working Party - Opinion 03/2017 on Processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS); http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610171.
[27] See GDPR, Article 4 (2).
[28] See GDPR, Article 4 (1).
[29] See GDPR, Article 4 (7) and the European Data Protection Board, Guidelines 07/2020 on the concepts of controller and processor in the GDPR (hereinafter - "Guidelines 07/2020").

regarding the functioning of the vehicle, insurance companies offering "*Pay As You Drive*" contracts, or vehicle manufacturers gathering data on the wear and tear affecting the vehicle's parts to improve its quality. Pursuant to art. 26 GDPR, two or more controllers can jointly determine the purposes and means of the processing and thus be considered as joint controllers. In this case, they have to clearly define their respective obligations, especially as regards the exercising of the rights of data subjects and the provision of information as referred to in art. 13 and 14 GDPR.

41. The **data processor** is any person who processes personal data for and on behalf of the data controller.[30] The data processor collects and processes data on instruction from the data controller, without using those data for its own purposes. As an example, in a number of cases, equipment manufacturers and automotive suppliers may process data on behalf of vehicle manufacturers (which does not imply they cannot be a data controller for other purposes). In addition to requiring data processors to implement appropriate technical and organisational measures in order to guarantee a security level that is adapted to risk, art. 28 GDPR sets out data processors' obligations.

42. The **recipient** means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.[31] As an example, a commercial partner of the service provider that receives from the service provider personal data generated from the vehicle is a recipient of personal data. Whether they act as a new data controller or as a data processor, they shall comply with all the obligations imposed by the GDPR.

43. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients[32]; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing. As an example, law enforcement authorities are authorised third parties when they request personal data as part of an investigation in accordance with European Union or Member State law.

[30] See GDPR, Article 4 (8) and the Guidelines 07/2020.
[31] See GDPR, Article 4 (9) and the Guidelines 07/2020.
[32] GDPR, Article 4 (9) and Recital 31.

1.5 Privacy and data protection risks

44. Article 29 Working Party has already expressed several concerns about Internet of Things (IoT) systems that can also apply to connected vehicles.[33] The issues relating to data security and control already stressed regarding IoT are even more sensitive in the context of connected vehicles, since it entails road safety concerns – and can impact the physical integrity of the driver – in an environment traditionally perceived as isolated and protected from external interferences.

45. Also, connected vehicles raises significant data protection and privacy concerns regarding the processing of location data as its increasingly intrusive nature can put a strain on the current possibilities to remain anonymous. The EDPB wants to place particular emphasis and raise stakeholders' awareness to the fact that the use of location technologies requires the implementation of specific safeguards in order to prevent surveillance of individuals and misuse of the data.

1.5.1 Lack of control and information asymmetry

46. Vehicle drivers and passengers may not always be adequately informed about the processing of data taking place in or through a connected vehicle. The information may be given only to the vehicle owner, who may not be the driver, and may also not be provided in a timely fashion. Thus, there is a risk that there are insufficient functionalities or options offered to exercise the control necessary for affected individuals to avail themselves of their data protection and privacy rights. This point is of importance since, during their lifetime, vehicles may belong to more than one owner either because they are sold or because they are being leased rather than purchased.

47. Also, communication in the vehicle can be triggered automatically as well as by default, without the individual being aware of it. In the absence of the possibility to effectively control how the vehicle and its connected equipment interact, it is bound to become extraordinarily difficult for the user to control the flow of data. It will be even more difficult to control its subsequent use, and thereby prevent potential function creep.

1.5.2 Quality of the user's consent

48. The EDPB underlines that, when the data processing is based on consent, all elements of valid consent have to be met which means that consent shall be free, specific and informed and constitutes an unambiguous indication of the data subject's wishes as interpreted in EDPB guidelines on consent.[34] Data controllers need to pay careful attention to the modalities of obtaining valid consent from different participants, such as car owners or car users. Such consent must be provided separately, for specific purposes and may not be bundled with the contract to buy or lease a new car. Consent must be as easily withdrawn as it is given.

49. The same has to be applied when consent is required to comply with the ePrivacy directive, for example if there is a storing of information or the gaining of access to information already stored in the vehicle as required in certain cases by art. 5(3) of the ePrivacy directive. Indeed, as outlined above, consent in this context has to be interpreted in light of the GDPR.

[33] Article 29 Working Party – Opinion 8/2014 on the Recent Developments on the Internet of Things; https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf.
[34] European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.1, 4 May 2020 (hereinafter - "Guidelines 05/2020").

50. In many cases, the user may not be aware of the data processing carried out in his/her vehicle. Such lack of information constitutes a significant barrier to demonstrating valid consent under the GDPR, as the consent must be informed. In such circumstances, consent cannot be relied upon as a legal basis for the corresponding data processing under the GDPR.

51. Classic mechanisms used to obtain individuals' consent may be difficult to apply in the context of connected vehicles, resulting in a "low-quality" consent based on a lack of information or in the factual impossibility to provide fine-tuned consent in line with the preferences expressed by individuals. In practice, consent might also be difficult to obtain for drivers and passengers who are not related to the vehicle's owner in the case of second-hand, leased, rented or borrowed vehicles.

52. When the ePrivacy directive does not require the data subject consent, the controller nonetheless has the responsibility of choosing the legal basis under art. 6 GDPR that is most appropriate to the case for the processing of personal data.

1.5.3 Further processing of personal data

53. When data is collected on the basis of consent as required by art. 5(3) of the ePrivacy directive or on one of the exemptions of art. 5(3), and subsequently processed in accordance with art. 6 GDPR, it can only be further processed either if the controller seeks additional consent for this other purpose or if the data controller can demonstrate that it is based on a Union or Member State law to safeguard the objectives referred to in art. 23 (1) GDPR[35]. The EDPB considers that further processing on the basis of a compatibility test according to art. 6(4) GDPR is not possible in such cases, since it would undermine the data protection standard of the ePrivacy directive. Indeed, consent, where required under the ePrivacy directive, needs to be specific and informed, meaning that data subjects must be aware of each data processing purpose and entitled to refuse specific ones[36]. Considering that further processing on the basis of a compatibility test according to art. 6(4) of the GDPR is possible would circumvent the very principle of the consent requirements set forth by the current directive.

54. The EDPB recalls that the initial consent will never legitimise further processing as consent needs to be informed and specific to be valid.

55. For instance, telemetry data, which is collected during use of the vehicle for maintenance purposes may not be disclosed to motor insurance companies without the users consent for the purpose of creating driver profiles to offer driving behaviour-based insurance policies.

56. Furthermore, data collected by connected vehicles may be processed by law enforcement authorities to detect speeding or other infractions if and when the specific conditions in the law enforcement directive are fulfilled. In this case, such data will be considered as relating to criminal convictions and offences under the conditions laid down by art. 10 GDPR and any applicable national legislation. Manufacturers may provide the law enforcement authorities with such data if the specific conditions for such processing are fulfilled. The EDPB points out that processing of personal data for the sole purpose of fulfilling requests made by law enforcement authorities does not constitute a specified, explicit and legitimate purpose within the meaning of art. 5(1)(b) GDPR. When law enforcement authorities are authorized by law, they could be third parties within the meaning of art. 4(10) GDPR, in this case

[35] See also European Data Protection Board, Guidelines 10/2020 on restrictions under Article 23 GDPR.
[36] Guidelines 05/2020, sections 3.2 and 3.3.

manufacturers would be entitled to provide them with any data at their disposal subject to compliance with the relevant legal framework in each Member State.

1.5.4 Excessive data collection

57. With the ever-increasing number of sensors being deployed in connected vehicles there is a very high risk of excessive data collection compared to what is necessary to achieve the purpose.

58. The development of new functionalities and more specifically those based on machine learning algorithms may require a large amount of data collected over a long period of time.

1.5.5 Security of personal data

59. The plurality of functionalities, services and interfaces (e.g., web, USB, RFID, Wi-Fi) offered by connected vehicles increases the attack surface and thus the number of potential vulnerabilities through which personal data could be compromised. Unlike most IoT devices, connected vehicles are critical systems where a security breach may endanger the life of its users and people around. The importance of addressing the risk of hackers attempting to exploit connected vehicles' vulnerabilities is thus heightened.

60. In addition, personal data stored on vehicles and/or at external locations (e.g., in cloud computing infrastructures) must be adequately secured against unauthorized access. For instance, during maintenance, a vehicle has to be handed to a technician who will require access to some of the vehicle's technical data. While the technician needs to have access to the technical data, there is a possibility that the technician could attempt to access all the data stored in the vehicle.

2 GENERAL RECOMMENDATIONS

61. In order to mitigate the risks for data subjects identified above, the following general recommendations should be followed by vehicle and equipment manufacturers, service providers or any other stakeholder who may act as data controller or data processor in relation to connected vehicles.

2.1 Categories of data

62. As noted in the introduction, most data associated with connected vehicles will be considered personal data to the extent that it is possible to link it to one or more identifiable individuals. This includes technical data concerning the vehicle's movements (e.g., speed, distance travelled) as well concerning the vehicle's condition (e.g., engine coolant temperature, engine RPM, tyre pressure). Certain data generated by connected vehicles may also warrant special attention given their sensitivity and/or potential impact on the rights and interests of data subjects. At present, the EDPB has identified three categories of personal data warranting special attention, by vehicle and equipment manufacturers, service providers and other data controllers: location data, biometric data (and any special category of data as defined in art. 9 GDPR) and data that could reveal offences or traffic violations.

2.1.1 Location data

63. When collecting personal data, vehicle and equipment manufacturers, service providers and other data controllers should keep in mind that location data are particularly revealing of the life habits of data subjects. The journeys carried out are very characteristic in that they

enable one to infer the place of work and of residence, as well as a driver's centres of interest (leisure), and may possibly reveal sensitive information such as religion through the place of worship, or sexual orientation through the places visited. Accordingly, the vehicle and equipment manufacturer, service provider and other data controller should be particularly vigilant not to collect location data except if doing so is absolutely necessary for the purpose of processing. As an example, when the processing consists in detecting the vehicle's movement, the gyroscope is sufficient to fulfil that function, without there being a need to collect location data.

64. In general, collecting location data is also subject to compliance with the following principles:

- adequate configuration of the frequency of access to, and of the level of detail of, location data collected relative to the purpose of processing. For example, a weather application should not be able to access the vehicle's location every second, even with the consent of the data subject;
- providing accurate information on the purpose of processing (e.g., is location history stored? If so, what is its purpose?);
- when the processing is based on consent, obtaining valid (free, specific and informed) consent that is distinct from the general conditions of sale or use, for example on the on-board computer;
- activating location only when the user launches a functionality that requires the vehicle's location to be known, and not by default and continuously when the car is started;
- informing the user that location has been activated, in particular by using icons (e.g., an arrow that moves across the screen);
- the option to deactivate location at any time;
- defining a limited storage period.

2.1.2 Biometric data

65. In the context of connected vehicles, biometric data used for the purpose of uniquely identifying a natural person may be processed, within the remit of art. 9 GDPR and the national exceptions, among other things, to enable access to a vehicle, to authenticate the driver/owner, and/or to enable access to a driver's profile settings and preferences. When considering the use of biometric data, guaranteeing the data subject full control over his or her data involves, on the one hand, providing for the existence of a non-biometric alternative (e.g., using a physical key or a code) without additional constraint (that is, the use of biometrics should not be mandatory), and, on the other hand, storing and comparing the biometric template in encrypted form only on a local basis, with biometric data not being processed by an external reading/comparison terminal.

66. In the case of biometric data[37], it is important to ensure that the biometric authentication solution is sufficiently reliable, in particular by complying with the following principles:

[37] The prohibition principle set out in article 9.1 GDPR only relates to "*biometric data for the purpose of uniquely identifying a natural person*".

– the adjustment of the biometric solution used (e.g., the rate of false positives and false negatives) is adapted to the security level of the required access control;

– the biometric solution used is based on a sensor that is resistant to attacks (such as the use of a flat-printed print for fingerprint recognition);

– the number of authentication attempts is limited;

– the biometric template/model is stored in the vehicle, in an encrypted form using a cryptographic algorithm and key management that comply with the state of the art;

– the raw data used to make up the biometric template and for user authentication are processed in real time without ever being stored, even locally.

2.1.3 Data revealing criminal offenses or other infractions

67. In order to process data that relate to potential criminal offences within the meaning of art. 10 GDPR, the EDPB recommends to resort to the local processing of the data where the data subject has full control over the processing in question (see discussion on local processing in section 2.4). Indeed – except for some exceptions (see the case study on accidentology studies presented below in section 3.3) – external processing of data revealing criminal offences or other infractions is forbidden. Thus, according to the sensitivity of the data, strong security measures such as those described in section 2.7 must be put in place in order to offer protection against the illegitimate access, modification and deletion of those data.

68. Indeed, some categories of personal data from connected vehicles could reveal that a criminal offence or other infraction has been or is being committed ("offence-related data") and therefore be subject to special restrictions (e.g., data indicating that the vehicle crossed a white line, the instantaneous speed of a vehicle combined with precise location data). Notably, in the event that such data would be processed by the competent national authorities for the purposes of criminal investigation and prosecution of criminal offence, the safeguards provided for in art. 10 GDPR would apply.

2.2 Purposes

69. Personal data may be processed for a wide variety of purposes in relation to connected vehicles, including driver safety, insurance, efficient transportation, entertainment or information services. In accordance with the GDPR, data controllers must ensure that their purposes are "specified, explicit and legitimate", not further processed in a way incompatible with those purposes and that there is a valid legal basis for the processing as required in art. 5 GDPR. Some concrete examples of purposes that may be pursued by data controllers operating in the context of connected vehicles are discussed in Part III of these guidelines, along with specific recommendations for each type of processing.

2.3 Relevance and data minimisation

70. To comply with the data minimization principle[38], vehicle and equipment manufacturers, service providers and other data controllers should pay special attention to the categories of data they need from a connected vehicle, as they shall only collect personal data that are relevant and necessary for the processing. For instance, location data are particularly intrusive and can reveal many life habits of the data subjects. Accordingly, industry participants should be particularly vigilant not to collect location data except if doing so is

[38] GDPR, Article 5(1)(c).

absolutely necessary for the purpose of processing (see discussion on location data above, in section 2.1).

2.4 Data protection by design and by default

71. Taking into account the volume and diversity of personal data produced by connected vehicles, the EDPB notes that data controllers are required to ensure that technologies deployed in the context of connected vehicles are configured to respect the privacy of individuals by applying the obligations of data protection by design and by default as required by art. 25 GDPR. Technologies should be designed to minimize the collection of personal data, provide privacy-protective default settings and ensure that data subjects are well informed and have the option to easily modify configurations associated with their personal data. Specific guidance on how manufacturers and service providers can comply with data protection by design and by default could be beneficial for the industry and third party application providers.

72. Certain general practices, described below, can also help mitigate the risks to the rights and freedoms of natural persons associated with connected vehicles[39].

2.4.1 Local processing of personal data

73. In general, vehicle and equipment manufacturers, service providers and other data controllers should, wherever possible, use processes that do not involve personal data or transferring personal data outside of the vehicle (i.e., the data is processed internally). The nature of connected vehicles however does present risks, such as the possibility of attacks on local processing by outside actors or local data being leaked by selling parts of the vehicle. Therefore, adequate attention and security measures should be taken into account to ensure that local processing shall remain local. This scenario offers the advantage of guaranteeing to the user the sole and full control of his/her personal data and, as such, it presents, "by design", less privacy risks especially by prohibiting any data processing by stakeholders without the data subject knowledge. It also enables the processing of sensitive data such as biometric data or data relating to criminal offenses or other infractions, as well as detailed location data which otherwise would be subject to stricter rules (see below). In the same vein, it presents fewer cybersecurity risks and involves little latency, which makes it particularly suited to automated driving-assistance functions. Some examples of this type of solution could include:

– eco-driving applications that process data in the vehicle in order to display eco-driving advice in real time on the on-board screen;

– applications that involve a transfer of personal data to a device such as a smartphone under the user's full control (via, for example, Bluetooth or Wi-Fi), and where the vehicle's data are not transmitted to the application providers or the vehicle manufacturers; this would include, for instance, coupling of smartphones to use the car's display, multimedia systems, microphone (or other sensors) for phone calls, etc., to the extent that the data collected remain under the control of the data subject and is exclusively used to provide the service he or she has requested;

– in-vehicle safety enhancing applications such as those that provide audible signals or vibrations of the steering wheel when a driver overtakes a car without indicating or straying over white

[39] See as well European Data Protection Board, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, adopted on 20 October 2020 (hereinafter - "Guidelines 4/2019").

lines or which provides alerts as to the state of the vehicle (e.g., an alert on the wear and tear affecting brake pads);

– applications for unlocking, starting, and/or activating certain vehicle commands using the driver's biometric data that is stored within the vehicle (such as a face or voice models or fingerprint minutiae).

74. Applications such as the above involve processing carried out for the performance of purely personal activities by a natural person (i.e., without the transfer of personal data to a data controller or data processor). Therefore, in accordance with art. 2(2) GDPR, **these applications fall outside the scope of the GDPR.**

75. However, if the GDPR does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity, it does apply to controllers or processors, which provide the means for processing personal data for such personal or household activities (car manufacturers, service provider, etc.) in accordance with recital 18 GDPR. Hence, when they are acting as data controller or data processor, they must develop secure in-car application and with due respect to the principle of privacy by design and by default. In any case, according to recital 78 GDPR, "*When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations*".[40] One the one hand, it will enhance the development of user-centric services and, on the other hand, it will facilitate and secure any further uses in the future which could fall back within the scope of the GDPR. More specifically, the EDPB recommends developing a secure in-car application platform, physically divided from safety relevant car functions so that the access to car data does not depend on unnecessary external cloud capabilities.

76. Local data processing should be considered by car manufacturers and service providers, whenever possible, to mitigate the potential risks of cloud processing, as they are underlined in the opinion on Cloud Computing released by the Article 29 Working Party.[41]

77. In general users should be able to control how their data are collected and processed in the vehicle:

– information regarding the processing must be provided in the driver's language (manual, settings, etc.);

– the EDPB recommends that only data strictly necessary for the functioning of the vehicle are processed by default. Data subjects should have the possibility to activate or deactivate the data processing for each other purpose and controller/processor and have the possibility to delete the data concerned, taking into account the purpose and the legal basis of the data processing ;

[40] For more recommendations on privacy by design and privacy by default see also Guidelines 4/2019.
[41] Article 29 Working Party – Opinion 5/2012 on Cloud Computing; https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf.

– data should not be transmitted to any third parties (i.e., the user has sole access to the data);

– data should be retained only for as long as is necessary for the provision of the service or otherwise required by Union or Member State law;

– data subjects should be able to delete permanently any personal data before the vehicles are put up for sale;

– data subjects should, where feasible, have a direct access to the data generated by these applications.

78. Finally, while it may not always be possible to resort to local data processing for every use-case, "hybrid processing" can often be put in place. For instance, in the context of usage-based insurance, personal data regarding driving behaviour (such as the force exerted on the brake pedal, mileage driven, etc.) could either be processed inside the vehicle or by the telematics service provider on behalf of the insurance company (the data controller) to generate numerical scores that are transferred to the insurance company on a defined basis (e.g. on a monthly basis). In this way, the insurance company does not gain access to the raw behavioural data but only to the aggregate score that is the result of the processing. This ensures that principles of data minimization are satisfied by design. This also means that users must have the ability to exercise their right when data are stored by other parties: for example, a user should have the ability to delete data stored in the systems of a car maintenance shop or dealership under the conditions of art.17 GDPR.

2.4.2 Anonymization and pseudonymisation

79. If the transmission of personal data outside the vehicle is envisaged, consideration should be given to anonymize them before being transmitted. When anonymising the controller should take into account all processing involved which could potentially lead to re-identification of data, such as the transmission of locally anonymised data. The EDPB recalls that the principles of data protection do not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable[42]. Once a dataset is truly anonymised and individuals are no longer identifiable, European data protection law no longer applies. As a consequence, anonymisation, where relevant, may be a good strategy to keep the benefits and to mitigate the risks in relation to connected vehicles.

80. As detailed in the opinion by the Article 29 Working Party on anonymization techniques, various methods can be used – sometimes in combination – in order to reach data anonymisation.[43]

81. Other techniques such as pseudonymisation[44] can help minimize the risks generated by the data processing, taking into account that in most cases, directly identifiable data are not necessary to achieve the purpose of the processing. Pseudonymisation, if reinforced by security safeguards, improves the protection of personal data by reducing the risks of

[42] See GDPR, Article 4 (1) and Recital 26.
[43] WP29 - Opinion 05/2014 on Anonymisation Techniques; https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.
[44] GDPR, Article 4 (5). Enisa report on December 03, 2019: https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices.

misuse. Pseudonymisation is reversible, unlike anonymisation, and pseudonymised data are considered as personal data subject to the GDPR.

2.4.3 Data protection impact assessments

82. Given the scale and sensitivity of the personal data that can be generated *via* connected vehicles; it is likely that processing – particularly in situations where personal data are processed outside of the vehicle - will often result in a high risk to the rights and freedoms of individuals. Where this is the case, industry participants will be required to perform a data protection impact assessment (DPIA) to identify and mitigate the risks as detailed in art. 35 and 36 GDPR. Even in the cases where a DPIA is not required, it is a best practice to conduct one as early as possible in the design process. This will allow industry participants to factor the results of this analysis into their design choices prior to the roll-out of new technologies.

2.5 Information

83. Prior to the processing of personal data, the data subject shall be informed of the identity of the data controller (e.g., the vehicle and equipment manufacturer or service provider), the purpose of processing, the data recipients, the period for which data will be stored, and the data subject's rights under the GDPR[45].

84. In addition, the vehicle and equipment manufacturer, service provider or other data controller should also provide the data subject with the following information, in clear, simple, and easily-accessible terms:

- the contact details of the data protection officer;
- the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- the explicit mention of the legitimate interests pursued by the data controller or by a third party, when such legitimate interests constitute the legal basis for processing;
- the recipients or categories of recipients of the personal data, if any;
- the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
- the existence of the right to withdraw consent at any time without affecting the lawfulness of processing based on consent before its withdrawal where the processing is based on consent;
- where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and safeguards used to transfer them;
- whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

[45] GDPR, Article 5 (1) (a) and 13. See also Article 29 Working Party, Guidelines on Transparency under Regulation 2016/679 (wp260rev.01), endorsed by the EDPB.

- the existence of automated decision-making, including profiling that produces legal effects concerning the data subject or similarly significantly affects the data subject, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. This could particularly be the case in relation to the provision of usage-based insurance to individuals;
- the right to lodge a complaint with a supervisory authority;
- information about further processing;
- In case of joint data controllership, clear and complete information about the responsibilities of each data controller.

85. In some cases, personal data is not collected directly from the individual concerned. For instance, a vehicle and equipment manufacturer may rely on a dealer to collect information about the owner of the vehicle in order to offer an emergency road side assistance service. When data have not been collected directly, the vehicle and equipment manufacturer, service provider or other data controller shall, in addition to the information mentioned above, also indicate the categories of personal data concerned, the source from which the personal data originate, and, if applicable, whether those data came from publicly accessible sources. That information must be provided by the controller within a reasonable period after obtaining the data, and **no later than the first of the following dates** in accordance with art. 14 (3) GDPR: (i) one month after the data are obtained, having regard to the specific circumstances in which the personal data are processed, (ii) upon first communication with the data subject, or (iii) if those data are transmitted to a third party, before the transmission of the data.

86. New information may also need to be provided to data subjects when they are taken care of by new data controller. A roadside assistance service that interacts with connected vehicles can be provided by different data controllers depending in which country or region the assistance is required. New data controllers should provide data subjects with the required information when data subjects cross borders and services that interact with connected vehicles are provided by new data controllers.

87. The information directed to the data subjects may be provided in layers[46], i.e. by separating two levels of information: on the one hand, first-level information, which is the most important for the data subjects, and, on the other hand, information that presumably is of interest at a later stage. The essential first-level information includes, in addition to the identity of the data controller, the purpose of the processing and a description of the data subject's rights, as well as any additional information on the processing which has the most impact on the data subject and processing which could surprise them. The EDPB recommends that, in the context of connected vehicles, the data subject should be made aware of all the recipients in the first layer of information. As stated in the WP29 guidelines on transparency, controllers should provide information on the recipients that is most meaningful for data subjects. In practice, this will generally be the named recipients, so that data subjects know exactly who has their personal data. If controllers cannot provide the names of the recipients, the information should be as specific as possible by indicating the

[46] See Article 29 Working Party, Guidelines on Transparency under Regulation 2016/679 (wp260rev.01), endorsed by the EDPB.

type of recipient (i.e. by reference to the activities it carries out), the industry, sector and sub-sector, and the location of the recipients.

88. The data subjects may be informed by concise and easily understandable clauses in the contract of sale of the vehicle, in the contract for the provision of services, and/or in any written medium, by using distinct documents (e.g., the vehicle's maintenance record book or manual) or the on-board computer.

89. Standardised icons could be used in addition to the information necessary, as required under art. 13 and 14 GDPR, to enhance transparency by potentially reducing the need for vast amounts of written information to be presented to a data subject. It should be visible in vehicles in order to provide, in relation to the planned processing, a good overview that is understandable, and clearly legible. The EDPB emphasises the importance of standardising those icons, so that the user finds the same symbols regardless of the make or model of the vehicle. For example, when certain types of data are being collected, such as location, the vehicles could have a clear signal on-board (such as a light inside the vehicle) to inform passengers about data collection.

2.6 Rights of the data subject

90. Vehicle and equipment manufacturers, service providers and other data controllers should facilitate data subjects' control over their data during the entire processing period, through the implementation of specific tools providing an effective way to exercise their rights, in particular their right of access, rectification, erasure, their right to restrict the processing and, depending on the legal basis of the processing, their right to data portability and their right to object.

91. To facilitate settings modifications, a profile management system should be implemented in order to store the preferences of known drivers and help them to change easily their privacy settings anytime. The profile management system should centralize every data setting for each data processing, especially to facilitate the access, deletion, removal and portability of personal data from vehicle systems at the request of the data subject. Drivers should be enabled to stop the collection of certain types of data, temporarily or permanently, at any moment, unless there is a specific legal ground that the controller can rely on to continue the collection of specific data. In case of a contract that provides a personalized offer based on driving behaviour this may mean that the user as a result should be reverted to the standard conditions of that contract. These features should be implemented inside the vehicle, although it could also be provided to data subjects through additional means (e.g., dedicated application). Furthermore, in order to allow data subjects to quickly and easily remove personal data that can be stored on the car's dashboard (for example, GPS navigation history, web browsing, etc.), the EDPB recommends that manufacturers provide a simple functionality (such as a delete button).

92. The sale of a connected vehicle and the ensuing change of ownership should also trigger the deletion of any personal data, which is no longer needed for the previous specified purposes and the data subject should be able to exercise his or her right to portability.

2.7 Security

93. Vehicle and equipment manufacturers, service providers and other data controllers should put in place measures that guarantee the security and confidentiality of processed data and

take all useful precautions to prevent control being taken by an unauthorised person. In particular, industry participants should consider adopting the following measures:

- encrypting the communication channels by means of a state-of-the-art algorithm;
- putting in place an encryption-key management system that is unique to each vehicle, not to each model;
- when stored remotely, encrypting data by means of state-of-the-art algorithms;
- regularly renewing encryption keys;
- protecting encryptions keys from any disclosure;
- authenticating data-receiving devices;
- ensuring data integrity (e.g., by hashing);
- make access to personal data subject to reliable user authentication techniques (password, electronic certificate, etc.);

94. Concerning more specifically vehicle manufacturers, the EDPB recommends the implementation of the following security measures:

- partitioning the vehicle's vital functions from those always relying on telecommunication capacities (e.g., "infotainment");
- implementing technical measures that enable vehicle manufacturers to rapidly patch security vulnerabilities during the entire lifespan of the vehicle;
- for the vehicle's vital functions, give priority as much as possible to using secure means of communications that are specifically dedicated to transportation;
- setting up an alarm system in case of attack on the vehicle's systems, with the possibility of operating in downgraded mode[47];
- storing a log history of any access to the vehicle's information system, e.g. going back six months as a maximum period, in order to enable the origin of any potential attack to be understood and periodically carry out a review of the logged information to detect possible anomalies.

95. These general recommendations should be completed by specific requirements taking into account the characteristics and purpose of each data processing.

2.8 Transmitting personal data to third parties

96. In principle, only the data controller and the data subject have access to the data generated by a connected vehicle. However, the data controller may transmit personal data to a commercial partner (recipient), to the extent that such transmission lawfully relies on one of the legal bases stated in art. 6 GDPR.

[47] Downgraded mode is a vehicle operating mode ensuring that the functions essential for the safe operation of the vehicle (i.e., minimum safety requirements) would be guaranteed, even if other less important functionalities would be deactivated (e.g., the operation of the geo-guidance device can be considered as non-essential, as opposed to the braking system).

97. In view of the possible sensitivity of the vehicle-usage data (e.g., journeys made, driving style), the EDPB recommends that the data subject's consent be systematically obtained before their data are transmitted to a commercial partner acting as a data controller (e.g., by ticking a box that is not pre-ticked, or, where technically possible, by using a physical or logical device that the person can access from the vehicle). The commercial partner in turn becomes responsible for the data that it receives, and is subject to all the provisions of the GDPR.

98. The vehicle manufacturer, service provider or other data controller can transmit personal data to a data processor selected to play a part in providing the service to the data subject, provided the data processor shall not use those data for its own purpose. Data controllers and data processors shall draw up a contract or other legal document specifying the obligations of each party and setting out the provisions of art. 28 GDPR.

2.9 Transfer of personal data outside the EU/EEA

99. When personal data is transferred outside the European Economic Area, special safeguards are foreseen to ensure that the protection travels with the data.

100. As a consequence, the data controller may transfer personal data to a recipient only to the extent that such transfer is in accordance with the requirements laid down in Chapter V GDPR.

2.10 Use of in-vehicle Wi-Fi technologies

101. Advances in cellular technology have made it possible to easily use the Internet on the road. While it is possible to get Wi-Fi connectivity in a vehicle through a smartphone hotspot or a dedicated device (OBD-II dongle, wireless modem or router, etc.), most manufacturers offer nowadays models that include a built-in cellular data connection and are also capable of creating Wi-Fi networks. Depending on the case, various aspects must be considered:

– The Wi-Fi connectivity is offered as a service by a road professional, such as a taxi driver for its customers. In this case, the professional or his/her company might be considered as an internet service provider (ISP), hence be subject to specific obligations and restrictions regarding the processing of his / her clients' personal data.

– The Wi-Fi connectivity is put in place for the sole use of the driver (at the exclusion of the driver and his/her passengers). In this case, the processing of personal data is considered to be purely personal or household activity in accordance with art. 2(2)(c) and recital 18 GDPR.

102. In general, the proliferation of Internet connection interfaces via Wi-Fi poses greater risks to the privacy of individuals. Indeed, through their vehicles, users become continuous broadcasters, and can therefore be identified and tracked. In order to prevent tracking, easy to operate opt-out options ensuring the service set identifier (SSID) of the on-board Wi-Fi network is not collected should therefore be put in place by the vehicle and equipment manufacturers.

3 CASE STUDIES

103. This section addresses five specific examples of processing in the context of connected vehicles, which correspond to scenarios likely to be encountered by stakeholders in the sector. The examples cover data processing that requires calculating power which cannot be mobilised locally in the vehicle, and/or the sending of personal data to a third party to carry out further analysis or to provide further functionality remotely. For each type of processing, this document specifies the intended purposes, the categories of data collected, the retention period of such data, the rights of data subjects, the security measures to be implemented, and the recipients of the information. In the case some of these fields are not described in the following, the general recommendations described in the previous part apply.

104. The examples chosen are non-exhaustive and are meant to be indicative of the variety of types of processing, legal bases, actors, etc. that might be engaged in the context of connected vehicles.

3.1 Provision of a service by a third party

105. Data subjects may contract with a service provider in order to obtain added-value services relating to their vehicle. For example, a data subject may enter into a usage-based insurance contract that offers reduced insurance premiums for less driving ("Pay As You Drive") or good driving behaviour ("Pay How You Drive") and which necessitates monitoring of driving habits by the insurance company. A data subject could also contract with a company that offers roadside assistance in the event of a breakdown and which entails the transmission of the vehicle's location to the company or with a service provider in order to receive

messages or alerts relating to the vehicle's functioning (e.g., an alert on the state of brake wear, or a reminder of the technical-inspection date).

3.1.1 Usage-based insurance

106. "Pay as you drive" is a type of usage-based insurance that tracks the driver's mileage and/or driving habits to differentiate and reward "safe" drivers by giving them lower premiums. The insurer will require the driver to install a built-in telematics service, a mobile application or activate a built-in module from manufacturing that tracks the miles covered and/or the driving behaviour (braking pattern, rapid acceleration, etc.) of the policy holder. The information gathered by the telematic device will be used to assign the driver scores in order to analyse what risks he/she may pose to the insurance company.

107. As usage-based insurance requires consent under art. 5(3) of the ePrivacy directive, the EDPB outlines that the policy holder must have the choice to subscribe to a non-usage-based insurance policy. Otherwise, consent would not be considered freely given, as the performance of the contract would be conditional on the consent. Further, art. 7(3) GDPR requires that a data subject must have the right to withdraw consent.

3.1.1.1 Legal basis

108. When the data is collected through a publicly available electronic communication service (for example *via* the SIM card contained in the telematics device), consent will be needed in order to gain access to information that is already stored in the vehicle as provided by art. 5(3) ePrivacy directive. Indeed, none of the exemptions provided by those provisions can apply in this context: the processing is not for the sole purpose of carrying out the transmission of a communication over an electronic communications network nor does it relate to an information society service explicitly requested by the subscriber or user. Consent could be collected at the time of the conclusion of the contract.

109. As regards the processing of personal data following the storage or access to the end-user's terminal equipment, the insurance company can rely on art. 6(1)(b) GDPR in this specific context provided it can establish both that the processing takes place in the context of a valid contract with the data subject and that processing is necessary in order that the particular contract with the data subject can be performed. Insofar as the processing is objectively necessary for the performance of the contract with the data subject, the EDPB considers that reliance upon art. 6(1)(b) GDPR would not have the effect of lowering the additional protection provided by art. 5(3) of the ePrivacy directive in this specific instance. That legal basis is materialised by the data subject signing a contract with the insurance company.

3.1.1.2 Data collected

110. There is two types of personal data to be considered:

- **commercial and transactional data**: data subject's identifying information, transaction-related data, data relating to means of payment, etc.;
- **usage data**: personal data generated by the vehicle, driving habits, location, etc.

111. The EDPB recommends that, as far as possible, and given that there is a risk that the data collected via the telematics-box could be misused to create a precise profile of the driver's movements, raw data regarding driving behaviour should be either processed:

- inside the vehicle in telematics boxes or in the user's smartphone so that the insurer only accesses the results data (e.g., a score relating to driving habits), not detailed raw data (see section 2.1);
- or by the telematics service provider on behalf of the controller (the insurance company) to generate numerical scores that are transferred to the insurance company on a defined basis. In this case, raw data and data directly relating to the identity of the driver must be separated. This means that the telematics service provider receives the real-time data, but does not know the names, licence plates, etc. of the policy holders. On the other hand, the insurer knows the names of policyholders, but only receives the scores and the total kilometres and not the raw data used to produce such scores.

112. Moreover, it has to be noted that if only the mileage is necessary for the performance of the contract, location data shall not be collected.

3.1.1.3 Retention period

113. In the context of data processing taking place for the performance of a contract (i.e. provision of a service), it is important to distinguish between two types of data before defining their respective retention periods:

- **commercial and transactional data:** those data can be retained in an active database for the full duration of the contract. At the end of the contract, they can be archived physically (on a separate medium: DVD, etc.) or logically (by authorisation management) in the event of possible litigation. Thereafter, at the end of the statutory limitation periods, the data shall be deleted or anonymised;
- **usage data:** usage data can be classified as raw data and aggregated data. As stated above, if possible, data controllers or processors should not process raw data. If it is necessary, raw data should be kept only as long as they are required to elaborate the aggregated data and to check the validity of that aggregation process. Aggregated data should be kept as long as it is necessary for the provision of the service or otherwise requested by a Union or Member State law.

3.1.1.4 Information and rights of data subjects

114. Prior to the processing of personal data, the data subject shall be informed according to art. 13 GDPR, in a transparent and understandable way. In particular, he or she must be informed of the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period. In this last case, the EDPB recommends to adopt a pedagogic approach to emphasize the difference between raw data and the score produced on this basis, stressing, when it is the case, that the insurer will only collect the result of the score where appropriate.

115. Where data are not processed inside the vehicle but by a telematics provider on behalf of the controller (the insurance company), the information could usefully mention that, in this case, the provider will not have access to data directly relating to the identity of the driver (such as names, licence plates, etc.). Also, considering the importance of informing data subjects as to the consequences of processing of their personal data and the fact that data subjects should not be taken by surprise by the processing of their personal data, the EDPB recommends that data subject should be informed of the existence of profiling and the consequences of such profiling even if it does not involve any automated decision-making as referred to in art. 22 GDPR.

116. Regarding the right of data subjects, they shall be specifically informed of the available means to exercise his or her right of access, rectification, restriction and erasure. Since raw data collected in this context are provided by the data subject (through specific forms or through his or her activity) and processed on the basis of art. 6(1)(b) GDPR (performance of a contract), the data subject is entitled to exercise his or her right to data portability. As emphasized in the guidelines on the right to data portability, the EDPB strongly recommends "that data controllers clearly explain the difference between the types of data that a data subject can receive through the rights of subject access and data portability".[48]

117. The information can be provided when the contract is signed.

3.1.1.5 Recipient:

118. The EDPB recommends that, as far as possible, the vehicle's usage data should be processed directly in telematics boxes, so that the insurer only accesses the results data (e.g. a score), not detailed raw data.

119. If a telematics service provider collects the data on behalf of the controller (the insurance company) to generate numerical scores, it does not need to know the identity of the driver (such as names, licence plates, etc.) of the policy holders.

3.1.1.6 Security:

120. General recommendations apply. See section 2.7.

3.1.2 Renting and booking a parking space

121. The owner of a parking place may want to rent it. For this, he/she lists a spot and sets a price for it on a web application. Then, once the parking spot is listed, the application notifies the owner when a driver wants to book it. The driver can select a destination and check for available parking spots based on multiple criteria. After the approval of the owner, the transaction is confirmed and the service provider handles the payment transaction then uses navigation to drive to the location.

3.1.2.1 Legal basis

122. When the data is collected through a publicly available electronic communication, art. 5(3) of the ePrivacy directive applies.

123. Because this is an information society service, art. 5(3) of the ePrivacy directive does not require consent for gaining access to information that is already stored in the vehicle when such a service is explicitly requested by the subscriber.

124. For the processing of personal data and only for data necessary for the performance of the contract to which the data subject is party, art. 6(1)(b) GDPR will be the legal basis.

3.1.2.2 Data collected

125. Data processed includes the driver contact details (name, email, telephone number, vehicle type (e.g. car, truck, motorcycle), license plate number, parking period, payment details (e.g. credit card info) as well as navigation data.

[48] Article 29 Working Party, Guidelines on the right to data portability under Regulation 2016/676, WP242 rev.01, endorsed by EDPB, p. 13.

3.1.2.3 Retention period

126. Data should be retained only as long as it is necessary to fulfil the parking contract or otherwise as provided by Union or Member State law. After that data is either anonymised or deleted.

3.1.2.4 Information and rights of data subjects

127. Prior to the processing of personal data, the data subject should be informed according to art. 13 GDPR, in a transparent and understandable way.

128. The data subject should be specifically informed of the available means to exercise his or her right of access, rectification, restriction and erasure. Since the data collected in this context are provided by the data subject (through specific forms or through his or her activity) and processed on the basis of art. 6(1)(b) GDPR (performance of a contract), the data subject is entitled to exercise his or her right to data portability. As emphasized in the guidelines on the right to data portability, the EDPB strongly recommends "*that data controllers clearly explain the difference between the types of data that a data subject can receive through the rights of subject access and data portability*".

3.1.2.5 Recipient:

129. In principle, only the data controller and the data processor have access to the data.

3.1.2.6 Security:

130. General recommendations apply. See section 2.7.

3.2 eCall

131. In the event of a serious accident in the European Union, the vehicle automatically triggers an eCall to 112, the EU-wide emergency number (see section 1.1 for further details) which allows an ambulance to be sent the place of the accident promptly according to Regulation (EU) 2015/758 of 29 April 2015 concerning type-approval requirements for the deployment of the eCall in-vehicle system based on the 112 service, and amending Directive 2007/46/EC (hereinafter - "Regulation (EU) 2015/758").

132. Indeed, the eCall generator installed inside the vehicle, which enables transmission via a public mobile wireless communications network initiates an emergency call, which is either triggered automatically by vehicle sensors or manually by the vehicle occupants only in the event of an accident. In addition to activation of the audio channel, the second event triggered automatically as a result of an accident consists in generating the Minimum Set of Data (MSD) and sending it to the public safety answering point (PSAP).

3.2.1 Legal basis

133. Regarding the application of the ePrivacy directive, two provisions have to be considered:

– art. 9 regarding location data other than traffic data which only applies to electronic communication services;

– art. 5(3) for the gaining access to information stored in the generator installed inside the vehicle.

134. Despite the fact that, in principle, those provisions require the consent of the data subject, Regulation (EU) 2015/758 constitutes a legal obligation to which the data controller is subject (the data subject has no genuine or free choice and will be unable to refuse the

processing of his/her data). Hence, Regulation (EU) 2015/758 overrides the need of the driver's consent for the processing of location data and the MSD.[49]

135. The legal basis of the processing of those data will be compliance with a legal obligation as provided for in art. 6(1)(c) GDPR (i.e., Regulation (EU) 2015/758).

3.2.2 Data collected

136. Regulation (EU) 2015/578 provides that data sent by the 112-based eCall in-vehicle system shall include only the minimum information as referred to in the standard EN 15722:2015 'Intelligent transport systems — eSafety — eCall minimum set of data (MSD)' including:

- the indication if eCall has been manually or automatically triggered;
- the vehicle type;
- the vehicle identification number (VIN);
- the propulsion type of the vehicle;
- the timestamp of the initial data message generation within the current eCall incident event;
- the last known vehicle latitude and longitude position determined at the latest moment possible before message generation;
- the vehicle's last known real direction of travel determined at the latest moment possible before message generation (only the last three locations of the vehicle).

3.2.3 Retention period

137. Regulation (EU) 2015/758 stipulates that data shall not be retained for longer than is needed for processing emergency situations. Those data shall be completely deleted when they are no longer needed for that purpose. Furthermore, in the internal memory of the eCall system, data shall be automatically and constantly deleted. Only the vehicle's last three positions can be stored, insofar as it is strictly necessary to specify the current position of the vehicle and the direction of travel at the time of the event.

3.2.4 Information and rights of data subjects

138. Art. 6 of the Regulation (EU) 2015/758 stipulates that manufacturers shall provide clear and complete information on data processing done using the eCall system. This information shall be provided in the owner's manual separately for the 112-based eCall in-vehicle system and any third-party service supported eCall systems prior to the use of the system. It includes:

- the reference to the legal basis for the processing;
- the fact that the 112-based eCall in-vehicle system is activated by default;
- the arrangements for data processing that the 112-based eCall in-vehicle system performs;

[49] It has to be noted that Article 8-1-f of the Council negotiation mandate for the proposal for an "ePrivacy" regulation does provide a specific exemption for eCall as consent is not needed when *"it is necessary to locate terminal equipment when an end-user makes an emergency communication either to the single European emergency number '112' or a national emergency number, in accordance with Article 13(3)."*

- the specific purpose of the eCall processing, which shall be limited to the emergency situations referred to in the first subparagraph of Art. 5(2) Regulation (EU) 2015/758;
- the types of data collected and processed and the recipients of that data;
- the time limit for the retention of data in the 112-based eCall in-vehicle system;
- the fact that there is no constant tracking of the vehicle;
- the arrangements for exercising data subjects' rights as well as the contact service responsible for handling access requests;
- any necessary additional information regarding traceability, tracking and processing of personal data in relation to the provision of a third-party service (TPS) eCall and/or other added value services, which shall be subject to explicit consent by the owner and in compliance with the GDPR. Particular account shall be taken of the fact that differences may exist between the data processing carried out through the 112-based eCall in-vehicle system and the TPS eCall in-vehicle systems or other added value services.

139. Furthermore, the service provider shall also provide the data subjects with information in accordance with art. 13 GDPR in a transparent and understandable way. In particular, he or she must be informed of the purposes of the processing for which the personal data are intended as well as the fact that the processing of personal data is based on a legal obligation to which the controller is subject.

140. In addition, taking into account the nature of the processing, the information about the recipients or categories of recipients of the personal data should be clear and the data subjects should be informed that the data are not be available outside the 112-based eCall in-vehicle system to any entities before the eCall is triggered.

141. Regarding rights of data subjects, it has to be noted that since the processing is based on a legal obligation, the right to object and the right to portability will not apply.

3.2.5 Recipient:

142. The data shall not be available outside the 112-based eCall in-vehicle system to any entities before the eCall is triggered.

143. When it is triggered (either manually by vehicle occupants or automatically as soon as an in-vehicle sensor detects a serious collision), the eCall system establishes a voice connection with the relevant PSAP and the MSD is sent to the PSAP operator.

144. Furthermore, data transmitted via the 112-based eCall in-vehicle system and processed by the PSAPs can be transferred to the emergency service and service partners referred to in Decision No 585/2014/EU only in the event of incidents related to eCalls and under the conditions set out in that Decision and are used exclusively for the attainment of the objectives of that Decision. Data processed by the PSAPs through the 112-based eCall in-vehicle system are not transferred to any other third parties without the explicit prior consent of the data subject.

3.2.6 Security

145. Regulation (EU) 2015/758 stipulates the requirements to incorporate into the eCall system technologies that strengthen the protection of privacy, in order to offer users the appropriate level of protection of privacy, as well as the guarantees needed to prevent

surveillance and abusive uses. In addition, manufacturers should ensure that the eCall system based on the number 112, as well as any other system providing an eCall that is handled by third-party services or an added-value service, are so designed that it is impossible for personal data to be exchanged between those systems.

146. Regarding PSAPs, Member States should ensure that personal data are protected against misuse, including unlawful access, alteration or loss, and that protocols concerning personal data storage, retention duration, processing and protection are established at the appropriate level and properly observed.

3.3 Accidentology studies

147. Data subjects may voluntarily agree to take part in accidentology studies aimed at better understanding the causes of road accidents and more generally scientific purposes.

3.3.1 Legal basis

148. When the data are collected through a public electronic communication service, the data controller will have to collect the consent of the data subject for the gaining of access to information that is already stored in the vehicle as provided by art. 5(3) of the ePrivacy directive. Indeed, none of the exemptions provided by those provisions can apply in this context: the processing is not for the sole purpose of carrying out the transmission of a communication over an electronic communications network nor does it relate to an information society service explicitly requested by the subscriber or user.

149. Regarding the processing of personal data and taking into account the variety and amount of personal data needed for accidentology studies, the EDPB recommends the processing to be based on the prior consent of the data subject according to art. 6 GDPR. Such prior consent must be provided on a specific form, through which the data subject volunteers to take part to the study and have his or her personal data processed for that purpose. Consent shall be an expression of the free, specific, and informed will of the person whose data are being processed (e.g., ticking a box that is not pre-ticked, or configuring the onboard computer to activate a function in the vehicle). Such consent must be provided separately, for specific purposes, may not be bundled with the contract to buy or lease a new car and the consent must be as easily withdrawn as it is given. Withdrawal of consent shall lead to the processing being stopped. The data shall then be deleted from the active database, or anonymised.

150. Consent required by art. 5(3) of the ePrivacy directive and consent needed as a legal basis for the processing of data can be collected at the same time (for example by checking a box clearly indicating what the data subject is consenting to).

151. It has to be noted that, depending on the conditions of the processing (nature of the data controller, etc.), another legal basis can be lawfully chosen as long as it does not lower the additional protection provided by art. 5(3) ePrivacy directive (see paragraph 15). If the processing is based on another legal basis such as the performance of a task carried out in the public interest (art. 6(1)(e) GDPR), the EDPB recommends that the data subjects are included in the study on a voluntary basis.

3.3.2 Data collected

152. The data controller shall only collect personal data that are strictly necessary for the processing.

153. There are two types of data to be considered:

– **data relating to participants and vehicles** ;

– **technical data from vehicles** (instantaneous speed, etc.).

154. Scientific research linked to accidentology justifies the collection of the instantaneous speed, including by legal persons who do not administer a public service in the strict sense.

155. Indeed, as noted above, the EDPB considers that instantaneous speed collected in the context of an accidentology study is not offence-related data by destination (i.e., it is not being collected for the purpose of investigating or prosecuting an offence), which justifies its collection by legal persons who do not administer a public service in the strict sense.

3.3.3 Retention period

156. It is important to distinguish between two types of data. First, the data relating to participants and vehicles can be retained for the duration of the study. Second, the technical data from vehicles should be retained for as short as possible for the purpose. In this regard, five years from the end date of the study appears to be a reasonable period. At the end of that period, the data shall be deleted or anonymised.

3.3.4 Information and rights of data subjects

157. Prior to the processing of personal data, the data subject shall be informed according to art. 13 GDPR, in a transparent and understandable way. In particular, in the case of collecting instantaneous speed, the data subjects should be specifically informed of the data collection. Since the data processing is based on consent, the data subject must be specifically informed of the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal. Moreover, because the data collected in this context are provided by the data subject (through specific forms or through his or her activity) and processed on the basis of art. 6(1)(a) GDPR (consent), the data subject is entitled to exercise his or her right to data portability. As emphasized in the guidelines on the right to data portability, the EDPB strongly recommends "that data controllers clearly explain the difference between the types of data that a data subject can receive through the rights of subject access and data portability". Consequently, the data controller should provide an easy way to withdraw his consent, freely and at any time, as well as develop tools to be able to answer data portability requests.

158. That information can be given upon signing the form to agree to take part in the accidentology study.

3.3.5 Recipient

159. In principle, only the data controller and the data processor have access to the data.

3.3.6 Security

160. As noted above, the security measures put in place shall be adapted to the level of data sensitivity. For instance, if instantaneous speed (or any other data related to criminal convictions and offences) is collected as part of the accidentology study, the EDPB strongly recommends putting in place strong security measures, such as:

– implementing pseudonymisation measures (e.g., secret-key hashing of data like the surname/first name of the data subject and the serial number);

– storing data relating to instantaneous speed and to location in separate databases (e.g., using a state-of-the-art encryption mechanism with distinct keys and approval mechanisms);

– and/or deleting location data as soon as the reference event or sequence is qualified (e.g., the type of road, day/night), and the storage of directly-identifying data in a separate database that can only be accessed by a small number of people.

3.4 Tackle auto theft

161. Data subjects may wish, in the case of theft, to attempt to find their vehicle using location. Using location data is limited to the strict needs of the investigation and to the case assessment by the competent legal authorities.

3.4.1 Legal basis

162. When the data is collected through a publicly available electronic communication service, art. 5(3) of the ePrivacy directive applies.

163. Because this is an information society service, art. 5(3) of the ePrivacy directive does not require consent for gaining access to information that is already stored in the vehicle when such a service is explicitly requested by the subscriber.

164. Regarding the processing of personal data, the legal basis for processing the location data will be the consent of the vehicle's owner, or, if applicable, the performance of a contract (only for data necessary for the performance of the contract to which the vehicle's owner is party).

165. Consent shall be an expression of the free, specific, and informed will of the person whose data are being processed (e.g. ticking a box that is not pre-ticked, or configuring the on-board computer to activate a function in the vehicle). Freedom to give consent involves the option of withdrawing consent at any time, of which the data subject should be expressly informed. Withdrawal of consent shall lead to the processing being stopped. The data should then be deleted from the active database, anonymised, or archived.

3.4.2 Data collected

166. Location data can only be transmitted as of the declaration of theft, and cannot be collected continuously the rest of the time.

3.4.3 Retention period

167. Location data can only be retained for the period during which the case is assessed by the competent legal authorities, or until the end of a procedure to dispel doubt that does not end with confirmation of the theft of the vehicle.

3.4.4 Information of the data subjects

168. Prior to the processing of personal data, the data subject should be informed according to art. 13 GDPR, in a transparent and understandable way. More specifically, the EDPB recommends that the data controller emphasizes that there is no constant tracking of the vehicle and that location data can only be collected and transmitted as of the declaration of theft. Moreover, the controller must provide the data subject with information relating to the fact that only approved officers of the remote-surveillance platform and legally approved authorities have access to the data.

169. Regarding the rights of the data subjects, when the data processing is based on consent, the data subject should be specifically informed of the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal. Besides, when the data collected in this context are provided by them (through specific forms or through his or her activity) and processed on the basis of art. 6(1)(a) (consent) or art. 6(1)(b) GDPR (performance of a contract), the data subject is entitled to exercise his or her right to data portability. As emphasized in the guidelines on the right to data portability, the EDPB strongly recommends "that data controllers clearly explain the difference between the types of data that a data subject can receive through the rights of subject access and data portability".

170. Consequently, the data controller should provide an easy way to withdraw his consent (only when consent is the legal basis), freely and at any time, as well as develop tools to be able to answer data portability requests.

171. The information can be provided when the contract is signed.

3.4.5 Recipients

172. In the event of a theft declaration, location data can be passed on the (i) approved officers of the remote-surveillance platform, and (ii) to the legally approved authorities.

3.4.6 Security

173. General recommendations apply. See section 2.7



Wytyczne 5/2019 w sprawie kryteriów dotyczących prawa do bycia zapomnianym w sprawach dotyczących wyszukiwarek internetowych na podstawie RODO

(część 1)

Wersja 2.0

Przyjęte 7 lipca 2020 r.

Historia wersji

Wersja 2.0	7 lipca 2020 r.	Przyjęcie wytycznych po przeprowadzeniu konsultacji publicznych
Wersja 1.1	17 lutego 2020 r.	Niewielkie zmiany
Wersja 1.0	2 grudnia 2019 r.	Przyjęcie wytycznych do konsultacji publicznych

Spis treści

Wprowadzenie 5

1 Prawne podstawy do żądania usunięcia z listy wyników wyszukiwania na podstawie RODO 8

1.1 Podstawa 1: Prawo do żądania usunięcia z listy wyników wyszukiwania, gdy dane osobowe nie są już niezbędne w związku z przetwarzaniem przez dostawcę wyszukiwarki internetowej (art. 17 ust. 1 lit. a)) 8

1.2 Podstawa 2: Prawo do żądania usunięcia z listy wyników wyszukiwania gdy osoba, której dane dotyczą, cofa zgodę, gdy podstawa prawna, na której opiera się przetwarzanie, jest zgodna z art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) RODO i nie ma innej podstawy prawnej przetwarzania (art. 17 ust. 1 lit. b)) 9

1.3 Podstawa 3: Prawo do żądania usunięcia z listy wyników wyszukiwania, gdy osoba, której dane dotyczą, korzysta ze swojego prawa sprzeciwu wobec przetwarzania jej danych osobowych (art. 17 ust. 1 lit. c)) 10

1.4 Podstawa 4: Prawo do żądania usunięcia z listy wyników wyszukiwania, gdy dane osobowe były przetwarzane niezgodnie z prawem (art. 17 ust. 1 lit. d)) 11

1.5 Podstawa 5: Prawo do żądania usunięcia z listy wyników wyszukiwania gdy dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego (art. 17 ust. 1 lit. e)) 12

1.6 Podstawa 6: Prawo do żądania usunięcia z listy wyników wyszukiwania gdy dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego dziecku (art. 17 ust. 1 lit. f)) 12

2 Wyjątki od prawa do żądania usunięcia z listy wyników wyszukiwania na podstawie art. 17 ust. 3 13

2.1 Przetwarzanie jest niezbędne do korzystania z prawa do wolności wypowiedzi i informacji 14

2.2 Przetwarzanie jest niezbędne do wywiązania się z prawnego obowiązku, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi 16

2.2.1 Obowiązek prawny 16

2.2.2 Wykonanie zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej 17

2.3 Względy interesu publicznego w dziedzinie zdrowia publicznego 18

2.4 Do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1, o ile prawdopodobne jest, że prawo, o którym mowa w ust. 1, uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania 19

2.5 Ustalanie, dochodzenie lub obrona roszczeń 19

Europejska Rada Ochrony Danych

uwzględniając art. 70 ust. 1 lit. e) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (zwanego dalej „RODO"),

uwzględniając Porozumienie EOG, a w szczególności jego załącznik XI i protokół 37, w brzmieniu zmienionym decyzją Wspólnego Komitetu EOG nr 154/2018 z dnia 6 lipca 2018 r.[1],

uwzględniając art. 12 i 22 swojego regulaminu wewnętrznego,

PRZYJMUJE NINIEJSZE WYTYCZNE:

WPROWADZENIE

1. Zgodnie z wyrokiem Trybunału Sprawiedliwości Unii Europejskiej („**TSUE**") w sprawie Costeja z dnia 13 maja 2014 r.[2], osoba, której dane dotyczą, może domagać się od dostawcy wyszukiwarki internetowej[3] usunięcia linku lub większej liczby linków do stron internetowych z listy wyników wyszukiwania wyświetlanej po wpisaniu w okno wyszukiwania jej imienia i nazwiska.
2. Zgodnie z raportem przejrzystości Google[4] odsetek adresów URL, które nie zostały usunięte z listy wyników wyszukiwania przez Google, nie zwiększył się w ciągu ostatnich pięciu lat od momentu wydania wspomnianego wyroku. Jednak wydaje się, że w następstwie wyroku TSUE osoby, których dane dotyczą, mają większą świadomość na temat przysługującego im prawa do wniesienia skargi dotyczącej odmowy usunięcia z listy wyników wyszukiwania, ponieważ organy nadzorcze zaobserwowały wzrost liczby skarg dotyczących odmowy usunięcia linków z listy wyników wyszukiwania ze strony dostawcy wyszukiwarki internetowej.
3. Europejska Rada Ochrony Danych („**EROD**"), zgodnie ze swoim planem działania, opracowuje wytyczne dotyczące art. 17 ogólnego rozporządzenia o ochronie danych („**RODO**"). Aż do momentu ich ukończenia organy nadzorcze muszą rozpatrywać i badać skargi wnoszone przez osoby, których dane dotyczą w możliwie największym zakresie i możliwie najbardziej terminowo.
4. Stosownie do powyższego, dokument ten ma na celu interpretację prawa do bycia zapomnianym w sprawach dotyczących wyszukiwarek internetowych w świetle art. 17 RODO („**prawo do żądania usunięcia z listy wyników wyszukiwania**"). Prawo do bycia zapomnianym istotnie ustanowiono w ramach art. 17 RODO, aby uwzględnić prawo do żądania usunięcia z listy wyników wyszukiwania ustanowione w wyroku w sprawie Costejy.
5. Niemniej, zgodnie z dyrektywą 95/46/WE z dnia 24 października 1995 r. („**dyrektywa**") oraz jak orzekł TSUE we wspomnianym powyżej wyroku w sprawie Costejy[5], prawo do żądania usunięcia z listy wyników wyszukiwania wiąże się z dwoma prawami (prawem do sprzeciwu i prawem do usunięcia danych ujętymi w RODO). W istocie wyraźnie przewidziano stosowanie art. 21 jako trzecią podstawę do prawa do usunięcia danych. W związku z tym zarówno art. 17, jak i art. 21 RODO mogą służyć jako podstawa prawna żądania usunięcia z listy wyników wyszukiwania. Prawo do sprzeciwu i prawo do usunięcia danych przysługiwały już na podstawie dyrektywy. Niemniej, jak zostanie to omówione, sformułowanie zawarte w RODO wymaga dostosowania dotyczącego interpretacji tych praw.
6. Przede wszystkim należy zauważyć, że chociaż art. 17 RODO stosuje się do wszystkich administratorów danych, w niniejszym dokumencie skupiono się na przetwarzaniu danych przez dostawców wyszukiwarek internetowych i żądaniach usunięcia z listy wyników wyszukiwania wnoszonych przez osoby, których dane dotyczą.
7. Istnieją pewne kwestie warte rozważenia przy stosowaniu art. 17 RODO względem przetwarzania danych przez dostawców wyszukiwarek internetowych. W tym względzie należy zaznaczyć, że konieczne jest rozróżnienie między przetwarzaniem danych osobowych w kontekście działalności dostawcy wyszukiwarki internetowej, a przetwarzaniem prowadzonym przez wydawców stron internetowych osób trzecich, takich jak media oferujące treść magazynów online[6].
8. Jeżeli osoba, której dane dotyczą, zdoła uzyskać usunięcie danych treści, będzie to oznaczało usunięcie tych konkretnych treści z listy wyników wyszukiwania wyników wyszukiwania dotyczących osoby, której dane dotyczą, przy wyszukiwaniu, co do zasady, na podstawie jej imienia i nazwiska. Treści te wciąż będą jednak dostępne przy wyszukiwaniu według innych kryteriów.
9. Żądanie usunięcia z listy wyników wyszukiwania nie skutkuje całkowitym usunięciem danych osobowych. Dane osobowe istotnie nie zostaną usunięte ani ze źródłowej strony internetowej ani z indeksu i pamięci podręcznej dostawcy wyszukiwarki internetowej. Osoba, której dane dotyczą, może na przykład dążyć do usunięcia danych osobowych z indeksu wyszukiwarki internetowej, które mają swoje źródło w mediach, takich jak artykuł prasowy. W takim przypadku link do danych osobowych może zostać usunięty z indeksu wyszukiwarki internetowej. Artykuł, o którym mowa, pozostanie jednak w zakresie kontroli mediów i może być nadal publicznie dostępny, nawet jeżeli nie będzie widoczny w wynikach wyszukiwania na podstawie zapytań zawierających co do zasady imię i nazwisko osoby, której dane dotyczą.
10. Dostawcy wyszukiwarek internetowych nie są jednak ogólnie zwolnieni z obowiązku całkowitego usunięcia. W niektórych szczególnych przypadkach będą oni musieli dokonać w swoich indeksach lub w pamięci podręcznej rzeczywistego i całkowitego usunięcia. Na przykład

[1] Odniesienia do „państw członkowskich" w niniejszych wytycznych należy rozumieć jako odniesienia do „państw członkowskich EOG".
[2] TSUE, sprawa C-131/12 Google Spain SL i Google Inc. przeciwko Agencia Española de Protección de Datos (AEPD) i Mariowi Costesze Gonzálezowi, wyrok z dnia 13 maja 2014 r.
[3] w tym od archiwów internetowych takich jak archive.org
[4] https://transparencyreport.google.com/eu-privacy/overview?hl=pl

[5] TSUE, sprawa C-131/12, wyrok z dnia 13 maja 2014 r., pkt 88: *Artykuł 12 lit. b) oraz art. 14 akapit pierwszy lit. a) dyrektywy 95/46 należy interpretować w ten sposób, że ustanowione w tych przepisach normy są przestrzegane, a przewidziane w nich warunki rzeczywiście spełnione wówczas, gdy operator wyszukiwarki internetowej jest zobowiązany do usunięcia z wyświetlanej listy wyników wyszukiwania mającego za punkt wyjścia imię i nazwisko danej osoby linków do publikowanych przez osoby trzecie stron internetowych zawierających dotyczące tej osoby informacje, również w przypadku gdy to imię czy nazwisko czy te informacje nie zostały uprzednio czy jednocześnie usunięte z tych stron internetowych i, w odpowiednim przypadku, nawet jeśli ich publikacja na tych stronach jest zgodna z prawem.*
[6] TSUE, sprawa C-131/12, wyrok z dnia 13 maja 2014 r.; Europejski Trybunał Praw Człowieka (ETPCz) „M.L. i W.W. p. Niemcom", wyrok z dnia 28 czerwca 2018 r.

w przypadku, gdy dostawcy wyszukiwarek internetowych przestaliby przestrzegać żądań plików robots.txt zastosowanych przez pierwotnego wydawcę, w rzeczywistości byliby zobowiązani do całkowitego usunięcia adresu URL do treści, w przeciwieństwie do usunięcia z listy wyników wyszukiwania, które odbywa się głównie na podstawie imienia i nazwiska osoby, której dane dotyczą.

11. Niniejszy dokument podzielono na dwa tematy. Pierwszy temat dotyczy podstaw, na które zgodnie z art. 17 ust. 1 RODO może powołać się osoba, której dane dotyczą, w swoim żądaniu usunięcia z listy wyników wyszukiwania skierowanym do dostawcy wyszukiwarki internetowej. Drugi temat dotyczy wyłączeń w zakresie prawa do żądania usunięcia z listy wyników wyszukiwania zgodnych z art. 17 ust. 3 RODO. Niniejszy dokument będzie uzupełniony o dodatek poświęcony ocenie kryteriów rozpatrywania skarg dotyczących odmowy usunięcia z listy wyników wyszukiwania.
12. Niniejszy dokument nie dotyczy art. 17 ust. 2[7] RODO. W artykule tym wymaga się od administratorów danych, którzy upublicznili dane osobowe, poinformowania administratorów, którzy ponownie wykorzystali te dane osobowe poprzez łącza do nich, ich kopie lub replikacje. Taki obowiązek informacyjny nie ma zastosowania do dostawców wyszukiwarek internetowych, gdy znajdą informacje zawierające dane osobowe opublikowane lub zamieszczone w Internecie przez osoby trzecie, indeksując je w sposób automatyczny, czasowo przechowując i udostępniając internautom w sposób uporządkowany zgodnie z określonymi preferencjami[8]. Ponadto nie wymaga się w tym przypadku od dostawców wyszukiwarek internetowych otrzymujących żądanie usunięcia z listy wyników wyszukiwania od osoby, której dane dotyczą, poinformowania osoby trzeciej, która upubliczniła te informacje w Internecie. Zobowiązanie takie ma nałożyć większą odpowiedzialność na pierwotnych administratorów i dążyć do zapobiegania mnożeniu inicjatyw osób, których dane dotyczą. W tym względzie ważne jest oświadczenie Grupy Roboczej Art. 29, w którym stwierdza ona, że dostawcy wyszukiwarek internetowych *nie powinni co do zasady informować webmasterów stron, których dotyczy usunięcie z listy wyników wyszukiwania, o tym, że dostęp do niektórych stron internetowych za pośrednictwem wyszukiwarki internetowej po wpisaniu konkretnych zapytań nie jest możliwy,* ponieważ *komunikat taki nie ma żadnej podstawy prawnej w prawie Unii dotyczącym ochrony danych osobowych*[9]. Planuje się sporządzenie również oddzielnych wytycznych dotyczących konkretnie art. 17 ust. 2 RODO.

[7] Rozporządzenie 2016/679 (RODO), art. 17 ust. 2: *Jeżeli administrator upublicznił dane osobowe, o na mocy ust. 1 ma obowiązek usunąć te dane osobowe, to – biorąc pod uwagę dostępną technologię i koszt realizacji – podejmuje rozsądne działania, w tym środki techniczne, by poinformować administratorów przetwarzających te dane osobowe, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje.*

[8] Zobacz TSUE, sprawa C-136/17, GC i inni przeciwko CNIL, wyrok z dnia 24 września 2019 r., pkt 35 oraz sprawa C-131/12, wyrok z dnia 13 maja 2014 r., pkt 41.

[9] Grupa Robocza Art. 29, „Guidelines on the implementation of the CJEU judgment on »Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González C-131/12«" [„Wytyczne w sprawie wykonania wyroku TSUE w sprawie »Google Spain i Inc przeciwko Agencia Española de Protección de Datos (AEPD) i Mariowi Costesze Gonzálezowi C-131/12«"], WP 225, 26 listopada 2014 r., s. 23.

1 PRAWNE PODSTAWY DO ŻĄDANIA USUNIĘCIA Z LISTY WYNIKÓW WYSZUKIWANIA NA PODSTAWIE RODO

13. Prawo do żądania usunięcia z listy wyników wyszukiwania przewidziane w art. 17 RODO nie zmienia wniosków wyroku w sprawie Costejy, w którym TSUE stwierdził, że żądanie usunięcia z listy wyników wyszukiwania opiera się na prawie do sprostowania/usunięcia i na prawie sprzeciwu, zgodnie z odpowiednio art. 12 i 14 dyrektywy.
14. W art. 17 ust. 1 określono ogólną zasadę dotyczącą usuwania danych w sześciu następujących przypadkach:

a. dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub były w inny sposób przetwarzane *(art. 17 ust.1 lit. a));*
b. osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie *(art. 17 ust. 1 lit. b));*
c. osoba, której dane dotyczą, korzysta ze swojego prawa sprzeciwu wobec przetwarzania jej danych osobowych, wnosząc sprzeciw na mocy art. 21 ust. 1 i 2 RODO;
d. dane osobowe były przetwarzane niezgodnie z prawem *(art. 17 ust. 1 lit. d));*
e. usunięcie danych jest zgodne z obowiązkiem prawnym *(art. 17 ust. 1 lit. e));*
f. dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego małoletniemu *(art. 17 ust. 1 lit. f) odnoszący się do art. 8 ust. 1)*.

15. Chociaż wszystkie podstawy określone w art. 17 teoretycznie mają zastosowanie w odniesieniu do usuwania z listy wyników wyszukiwania, niektóre z nich będą w praktyce stosowane rzadko lub nie będą stosowane nigdy, tak jak w przypadku cofnięcia zgody (zob. podstawa 2 poniżej).
16. Osoba, której dane dotyczą, mogłaby jednak skierować żądanie o usunięcie z listy wyników wyszukiwania do dostawcy wyszukiwarki internetowej w oparciu o więcej niż jedną podstawę. Osoba, której dane dotyczą, mogłaby na przykład zażądać usunięcia z listy wyników wyszukiwania, ponieważ uważa, że przetwarzanie jej danych osobowych przez wyszukiwarkę internetową nie jest już niezbędne (art. 17 ust. 1 lit. a)), korzystając jednocześnie ze swojego prawa sprzeciwu względem przetwarzania zgodnie z art. 21 ust. 1 RODO (art. 17 ust. 1 lit. c)).
17. Aby organy nadzorcze mogły ocenić skargi dotyczące dostawców wyszukiwarek internetowych, którzy odmówili usunięcia konkretnych wyników wyszukiwania zgodnie z art. 17 RODO, powinny one ustalić, czy treść, do której odnosi się adres URL, powinna zostać usunięta z listy wyników wyszukiwania. Powinny zatem uwzględnić w swojej analizie merytorycznej skargi charakter treści udostępnionej przez wydawców stron internetowych osób trzecich.

1.1 Podstawa 1: Prawo do żądania usunięcia z listy wyników wyszukiwania, gdy dane osobowe nie są już niezbędne w związku z przetwarzaniem przez dostawcę usług wyszukiwania (art. 17 ust. 1 lit. a))

18. Zgodnie z art. 17 ust. 1 lit. a) RODO osoba, której dane dotyczą, może w związku z przeprowadzeniem wyszukiwania mającego co do zasady za punkt wyjścia jej imię i nazwisko zażądać od dostawcy wyszukiwarki internetowej usunięcia z listy wyników wyszukiwania

treści, jeżeli dane osobowe osoby, której dane dotyczą, wyświetlone na skutek tego wyszukiwania nie są już niezbędne do celów przetwarzania przez wyszukiwarkę internetową.

19. Przepis ten umożliwia osobie, której dane dotyczą, żądanie usunięcia z listy wyników wyszukiwania dotyczących jej danych osobowych, które są dostępne dłużej niż jest to niezbędne do celów przetwarzania dostawcy wyszukiwarki internetowej. Przetwarzanie takie odbywa się głównie w celu ułatwienia dostępności tych informacji dla użytkowników Internetu. W kontekście prawa do żądania usunięcia z listy wyników wyszukiwania należy uwzględnić równowagę między ochroną prywatności, a interesem internautów w dostępie do informacji. Należy w szczególności ocenić, czy z czasem dane osobowe się nie zdezaktualizowały lub czy nie zostały zaktualizowane.
20. Osoba, której dane dotyczą, może na przykład skorzystać ze swojego prawa do żądania usunięcia z listy wyników wyszukiwania zgodnie z art. 17 ust. 1 jeżeli:

- informacje o niej posiadane przez przedsiębiorstwo zostały usunięte z publicznego rejestru;
- link do strony internetowej firmy zawiera jej dane kontaktowe, mimo że nie pracuje już w tej firmie;
- informacje muszą być opublikowane w Internecie, aby spełnić obowiązek prawny, i pozostały online dłużej, niż przewidziano w przepisach.

21. Jak wskazano w przykładach, osoba, której dane dotyczą, może w szczególności zażądać usunięcia z listy wyników wyszukiwania treści, w których dane osobowe są wyraźnie nieprawidłowe z uwagi na upływ czasu lub zdezaktualizowane. Ocena taka będzie przy tym zależała od celów pierwotnego przetwarzania. W związku z tym organy nadzorcze w swojej analizie żądań o usunięcie z listy wyników wyszukiwania zgodnie z art. 17 ust. 1 lit. a) RODO powinny również uwzględniać w miarę dostępności pierwotny okres zatrzymywania danych osobowych.

1.2 Podstawa 2: Prawo do żądania usunięcia z listy wyników wyszukiwania gdy osoba, której dane dotyczą, cofa zgodę, gdy podstawa prawna, na której opiera się przetwarzanie, jest zgodna z art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) RODO i nie ma innej podstawy prawnej przetwarzania (art. 17 ust. 1 lit. b))

22. Zgodnie z art. 17 ust. 1 lit. b) RODO osoba, której dane dotyczą, może uzyskać usunięcie swoich danych osobowych, jeżeli cofnie zgodę na przetwarzanie.
23. W przypadku usunięcia z listy wyników wyszukiwania oznaczałoby to, że dostawca wyszukiwarki internetowej korzystałby ze zgody osoby, której dane dotyczą, jako zgodnej z prawem podstawy przetwarzania przez niego danych. W art. 17 ust. 1 RODO istotnie podnoszona jest kwestia zgodnej z prawem podstawy przetwarzania, na której opiera się dostawca wyszukiwarki internetowej do celów wyświetlania wyników wyszukiwania zawierających dane osobowe.
24. Z tego powodu wydaje się mało prawdopodobne, aby osoba, której dane dotyczą, kierowała żądanie usunięcia z listy wyników wyszukiwania na podstawie chęci cofnięcia zgody, gdyż administratorem danych, względem którego osoba, której dane dotyczą, wyraziła zgodę jest wydawca strony internetowej, nie zaś operator wyszukiwarki internetowej indeksującej dane. Interpretację tę poparł TSUE w swoim wyroku C-136/17 z dnia 24 września 2019 r. („**wyrok w sprawie Google 2**”)[10]. Trybunał wskazuje, że *(…) zgoda taka musi być „konkretna”, a zatem dotyczyć konkretnie przetwarzania dokonywanego w ramach działania wyszukiwarki (…). Jednakże w praktyce trudno jest sobie wyobrazić (…) aby operator wyszukiwarki przed przystąpieniem do przetwarzania danych osobowych ubiegał się, dla potrzeb swojej działalności w zakresie odsyłania do stron internetowych, o wyraźną zgodę osób, których te dane dotyczą. W każdym razie, (…) sam fakt, że dana osoba wnosi żądanie o usunięcie linków, oznacza co do zasady, że przynajmniej w dniu złożenia tego żądania osoba ta nie wyraża już zgody na przetwarzanie danych przez operatora wyszukiwarki.*

25. Niemniej, w przypadku wycofania zgody przez osobę, której dane dotyczą, na wykorzystywanie jej danych na konkretnej stronie internetowej, pierwotny wydawca tej strony internetowej powinien poinformować dostawców wyszukiwarek internetowych, którzy indeksowali te dane zgodnie z art. 17 ust. 2 RODO. Osoba, której dane dotyczą, wciąż byłaby uprawniona do uzyskania usunięcia jej danych osobowych z listy wyników wyszukiwania, lecz w takim przypadku zgodnie z art. 17 ust. 1 lit. c).

1.3 Podstawa 3: Prawo do żądania usunięcia z listy wyników wyszukiwania, gdy osoba, której dane dotyczą, korzysta ze swojego prawa sprzeciwu wobec przetwarzania jej danych osobowych (art. 17 ust. 1 lit. c))

26. Zgodnie z art. 17 ust. 1 lit. c) RODO osoba, której dane dotyczą, może uzyskać od dostawcy wyszukiwarki internetowej usunięcie jej danych osobowych, jeżeli wyraża sprzeciw wobec przetwarzania zgodnie z art. 21 ust. 1 RODO i jeżeli nie istnieją żadne nadrzędne zgodne z prawem podstawy przetwarzania przez administratora danych.
27. Prawo sprzeciwu przyznaje osobom, których dane dotyczą, silniejsze zabezpieczenia, gdyż nie ogranicza ono podstaw, zgodnie z którymi osoby, których dane dotyczą, mogą żądać usunięcia z listy wyników wyszukiwania, jak ma to miejsce w przypadku działania na podstawie art. 17 ust. 1 RODO.
28. Prawo sprzeciwu wobec przetwarzania przewidziano w art. 14 dyrektywy[11] i stanowi ono podstawę żądania usunięcia z listy wyników wyszukiwania od momentu wydania wyroku w sprawie Costejy. Różnice w sformułowaniu między art. 21 RODO a art. 14 dyrektywy sugerują jednak, że może również istnieć różnica w ich stosowaniu.
29. Na podstawie dyrektywy żądanie osoby, której dane dotyczą, musiało wynikać z *ważnych i uzasadnionych przyczyn wynikających z jego konkretnej sytuacji*. W przypadku RODO osoba, której dane dotyczą, może sprzeciwić się przetwarzaniu *z przyczyn związanych z jej szczególną sytuacją*. Nie musi już ona zatem wykazywać *ważnych i uzasadnionych przyczyn.*
30. RODO przenosi zatem ciężar dowodu, zapewniając domniemanie z korzyścią dla osoby, której dane dotyczą, nakładając dla odmiany obowiązek wykazania *ważnych prawnie uzasadnionych podstaw do przetwarzania* na administratora (art. 21 ust. 1). W związku z tym gdy dostawca wyszukiwarki internetowej otrzymuje żądanie usunięcia z listy wyników wyszukiwania oparte na szczególnej sytuacji osoby, której dane dotyczą, musi w takim przypadku usunąć takie dane

[10] TSUE, sprawa C–136/17, Commission nationale de l'informatique et des libertés (CNIL) przeciwko Google LLC, wyrok z dnia 24 września 2019 r.

[11] Dyrektywa 95/46/WE, art. 14: *Państwa członkowskie przyznają osobie, której dane dotyczą, prawo: a) przynajmniej w przypadkach wymienionych w art. 7 lit. e) i f), w dowolnym czasie z ważnych i uzasadnionych przyczyn wynikających z jego konkretnej sytuacji, sprzeciwu co do przetwarzania dotyczących jej danych, z zastrzeżeniem odmiennych postanowień ustawodawstwa krajowego. W przypadku uzasadnionego sprzeciwu przetwarzanie danych przez administratora danych nie może już obejmować tych danych.*

osobowe zgodnie z art. 17 ust. 1 lit. c) RODO, chyba że jest w stanie wykazać *nadrzędne prawnie uzasadnione podstawy* ujęcia konkretnych wyników wyszukiwania w liście wyników wyszukiwania, które czytane w związku z art. 21 ust. 1 świadczą o istnieniu *ważnych prawnie uzasadnionych podstaw (...), nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą*. Dostawca wyszukiwarki internetowej może ustanowić dowolne *nadrzędne prawnie uzasadnione podstawy,* w tym jakiekolwiek wyłączenia przewidziane w art. 17 ust. 3 RODO. Jeżeli dostawca wyszukiwarki internetowej nie wykaże jednak istnienia nadrzędnych prawnie uzasadnionych podstaw, osoba, której dane dotyczą, ma prawo uzyskać usunięcie z listy wyników wyszukiwania zgodnie z art. 17 ust. 1 lit. c) RODO. W istocie obecnie żądania usunięcia z listy wyników wyszukiwania wiążą się z sugestią osiągnięcia równowagi między powodami związanymi ze szczególną sytuacją osoby, której dane dotyczą, a ważnymi prawnie uzasadnionymi podstawami ze strony dostawcy wyszukiwarki internetowej. Istotna przy dokonywaniu takiej oceny może być równowaga między ochroną prywatności a interesami internautów w dostępie do informacji, jak stwierdził Trybunał w swoim wyroku w sprawie Costejy, jak również równowaga stosowana przez Europejski Trybunał Praw Człowieka w sprawach dotyczących prasy.

31. W związku z tym dostawcy wyszukiwarek internetowych i organy nadzorcze wciąż mogą do celów oceny żądań usunięcia z listy wyników wyszukiwania na podstawie prawa sprzeciwu (art. 17 ust. 1 lit. c) RODO) stosować kryteria dotyczące usunięcia z listy wyników wyszukiwania opracowane przez Grupę Roboczą Art. 29 w wytycznych dotyczących wykonania wyroku Trybunału Sprawiedliwości Unii Europejskiej *w* sprawie „Google Spain and Inc przeciwko Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12.
32. W tym względzie *szczególna sytuacja* osoby, której dane dotyczą, będzie leżała u podstaw żądania usunięcia z listy wyników wyszukiwania (na przykład wyniki wyszukiwania przynoszą szkodę osobie, której dane dotyczą, gdy ubiega się ona o pracę, lub niszczą jej reputację w życiu prywatnym) i zostanie ona uwzględniona przy ustalaniu równowagi między prawami osobistymi i prawem do informacji, poza zwykłymi kryteriami służącymi rozpatrywaniu żądań o usunięcie z listy wyników wyszukiwania, takimi jak:
    - osoba nie pełni żadnej roli w życiu publicznym;
    - informacje, których dotyczy żądanie, nie są związane z jej życiem zawodowym, lecz mają wpływ na jej prywatność;
    - informacje stanowią nawoływanie do nienawiści, pomówienie, znieslawienie w formie pisemnej lub podobne przestępstwo w obszarze wypowiedzi skierowanych przeciwko niej uznane za takie na podstawie orzeczenia sądowego;
    - dane wydają się być zweryfikowanymi faktami, lecz w rzeczywistości są nieprawidłowe;
    - dane odnoszą się do stosunkowo nieznacznego wykroczenia, które miało miejsce dawno temu i jest powodem uprzedzeń względem osoby, której dane dotyczą.
33. Niemniej nie będzie konieczności badania tych kryteriów przy braku dowodu świadczącego o ważnych prawnie uzasadnionych podstawach odmowy żądania.

1.4 Podstawa 4: Prawo do żądania usunięcia z listy wyników wyszukiwania, gdy dane osobowe były przetwarzane niezgodnie z prawem (art. 17 ust. 1 lit. d))

34. Zgodnie z art. 17 ust. 1 lit. d) RODO osoba, której dane dotyczą, może żądać usunięcia swoich danych osobowych, jeżeli były one przetwarzane niezgodnie z prawem.

35. W pierwszej kolejności należy zinterpretować pojęcie niezgodnego z prawem przetwarzania w świetle przepisów art. 6 RODO dotyczącego zgodności przetwarzania z prawem. Do interpretacji takiej mogą posłużyć inne przepisy ustanowione w ramach RODO (takie jak zasady z art. 5 RODO lub inne przepisy ujęte w rozdziale II).
36. Następnie należy poddać to pojęcie głębszej interpretacji jako naruszenie przepisów prawnych innych niż RODO. Interpretacji takiej muszą dokonać organy nadzorcze, zachowując obiektywność, zgodnie z przepisami prawa krajowego i z orzeczeniem sądu. Na przykład należy pozytywnie rozpatrzyć żądanie usunięcia z listy wyników wyszukiwania w przypadku, gdy ujmowanie danych osobowych w wykazie zostało wyraźnie zakazane orzeczeniem sądowym.

W przypadkach, gdy dostawca wyszukiwarki internetowej nie jest w stanie wykazać podstawy prawnej przetwarzania, żądanie usunięcia z listy wyników wyszukiwania może wejść w zakres stosowania art. 17 ust. 1 lit. d) RODO, gdyż przetwarzanie danych osobowych musi zostać w takich przypadkach uznane za niezgodne z prawem. Należy jednak przypomnieć, że w przypadku braku zgodności z prawem pierwotnego przetwarzania osoba, której dane dotyczą, wciąż ma prawo żądania usunięcia z listy wyników wyszukiwania na podstawie art. 17 ust. 1 lit. c) RODO.

1.5 Podstawa 5: Prawo do żądania usunięcia z listy wyników wyszukiwania gdy dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego (art. 17 ust. 1 lit. e))

37. Zgodnie z art. 17 ust. 1 lit. e) RODO osoba, której dane dotyczą, może żądać od dostawcy wyszukiwarki internetowej usunięcia wyniku lub wyników wyszukiwania, jeżeli dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega dostawca wyszukiwarki internetowej.
38. Wywiązanie się z obowiązku prawnego może wynikać z nakazu sądowego, wyraźnego zobowiązania wynikającego z prawa Unii lub prawa krajowego do podlegania „obowiązkowi prawnemu usunięcia" lub ze zwykłego naruszenia przez dostawcę usług wyszukiwania zbioru zatrzymywania. Do celów ilustracyjnych okres zatrzymywania danych jest ustalony dokumentem, nie byłby jednak przestrzegany (hipoteza ta dotyczy jednak głównie zbiorów publicznych). Przypadek ten mógłby obejmować hipotezę niezanonimizowanych danych lub danych, które umożliwiają identyfikację, dostępnych w ramach otwartych danych.

1.6 Podstawa 6: Prawo do żądania usunięcia z listy wyników wyszukiwania gdy dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego dziecku (art. 17 ust. 1 lit. f))

39. Zgodnie z art. 17 ust. 1 lit. f) RODO osoba, której dane dotyczą, może zażądać od dostawcy wyszukiwarki internetowej usunięcia z listy wyników wyszukiwania wyniku lub wyników wyszukiwania, jeżeli dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego dziecku, o którym mowa w art. 8 ust. 1 RODO.
40. Artykuł ten dotyczy bezpośredniego świadczenia usług społeczeństwa informacyjnego i żadnych innych rodzajów przetwarzania. W RODO nie zdefiniowano usług społeczeństwa

informacyjnego; odniesiono się raczej do definicji istniejących już w prawie Unii[12]. Istnieją pewne trudności interpretacyjne, gdyż w motywie 18 dyrektywy 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. przedstawiono szeroką i niejednoznaczną definicję pojęcia *bezpośredniego świadczenia usług społeczeństwa informacyjnego*. Wskazuje ona głównie, że usługi te *obejmują szeroki zakres rodzajów działalności gospodarczej prowadzonych w trybie on-line*, doprecyzowuje jednak, że nie ograniczają się one do *usług dających sposobność do zawierania umów on-line, ale, **o ile stanowią one działalność gospodarczą**, dotyczą także usług, które nie są wynagradzane przez tych, którzy je otrzymują, takie jak usługi polegające na oferowaniu informacji on-line lub informacji handlowych lub zapewniających narzędzia umożliwiające szukanie, dostęp oraz pozyskiwanie danych*, wymieniając kryteria działalności gospodarczej.

41. Z powyższego wynika, że istnieje duże prawdopodobieństwo, iż działania dostawców wyszukiwarek internetowych wchodzą w zakres bezpośredniego świadczenia usług społeczeństwa informacyjnego. Niemniej dostawcy wyszukiwarek internetowych nie ustalają czy indeksowane przez nich dane osobowe dotyczą dziecka. Mając jednak na uwadze ich szczególne obowiązki, i podlegając stosowaniu art. 17 ust. 3 RODO, musieliby oni usunąć z listy wyników wyszukiwania treści związane z dzieckiem zgodnie z art. 17 ust. 1 lit. c) RODO, uznając, że bycie dzieckiem jest ważną „przyczyną związaną ze szczególną sytuacją" (art. 21 RODO), oraz że *„szczególnej ochrony danych osobowych wymagają dzieci"* (motyw 38 RODO). W takim przypadku należy uwzględnić kontekst gromadzenia danych osobowych przez pierwotnego administratora. Gdy osoba, której dane dotyczą, żąda usunięcia treści z listy wyników wyszukiwania, należy w szczególności uwzględnić datę rozpoczęcia przetwarzania danych przez pierwotną stronę internetową.

2 WYJĄTKI OD PRAWA DO ŻĄDANIA USUNIĘCIA Z LISTY WYNIKÓW WYSZUKIWANIA NA PODSTAWIE ART. 17 UST. 3

42. Artykuł 17 ust. 3 RODO stanowi, że ust. 1 i 2 nie będą miały zastosowania, jeżeli przetwarzanie jest niezbędne:

a. do korzystania z prawa do wolności wypowiedzi i informacji *(art. 17 ust. 3 lit. a));*
b. do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi *(art. 17 ust. 3 lit. b));*
c. z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego zgodnie z art. 9 ust. 2 lit. h) oraz i) i art. 9 ust. 3 *(art. 17 ust. 3 lit. c));*
d. do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1, o ile prawdopodobne jest, że prawo, o którym mowa w ust. 1, uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania *(art. 17 ust. 3 lit. d));* lub
e. do ustalenia, dochodzenia lub obrony roszczeń *(art. 17 ust. 3 lit. e))*.

[12] Konkretnie art. 1 ust. 1 lit. b) dyrektywy (UE) 2015/1535 Parlamentu Europejskiego i Rady z dnia 9 września 2015 r. ustanawiającej procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego (ujednolicenie).

43. Część ta ma na celu wykazanie, że nie wydaje się, aby większość wyjątków z art. 17 ust. 3 RODO była odpowiednia w przypadku żądania usunięcia z listy wyników wyszukiwania. Taka nieadekwatność działa na korzyść stosowania art. 21 RODO do celów żądania usunięcia z listy wyników wyszukiwania. W każdym razie należy pamiętać, że na wyjątki przewidziane w art. 17 ust 3 RODO można powoływać się jako na ważne prawnie uzasadnione podstawy zgodnie z art. 17 ust. 1 lit. c) RODO.

2.1 Przetwarzanie jest niezbędne do korzystania z prawa do wolności wypowiedzi i informacji

44. To odstępstwo od stosowania art. 17 ust. 1 RODO należy interpretować i stosować w kontekście charakterystycznych cech definiujących usunięcie. Artykuł 17 ust. 1 RODO opisuje się jako wyraźne i bezwarunkowe uprawnienie skierowane do administratorów. W przypadku spełnienia warunków określonych w art. 17 ust. 1 RODO administrator *ma obowiązek bez zbędnej zwłoki usunąć dane osobowe*. Prawo to nie jest jednak prawem bezwzględnym. Wyłączenia ujęte w art. 17 ust. 3 RODO wskazują przypadki, w których obowiązek ten nie ma zastosowania.
45. Równowaga między ochroną praw zainteresowanych stron a wolnością wypowiedzi, w tym swobodnego dostępu do informacji, stanowi jednak nieodłączną część art. 17 RODO.
46. TSUE uznał w wyroku w sprawie Costeja i powtórzył ostatnio w wyroku w sprawie Google 2, że przetwarzanie dokonywane przez dostawcę usług wyszukiwania może znacząco oddziaływać na prawa podstawowe do poszanowania prywatności i na przepisy o ochronie danych, gdy wyszukiwanie jest prowadzone po wpisaniu w kryteria wyszukiwania głównie imienia i nazwiska osoby, której dane dotyczą.
47. Ważąc prawa i wolności osób, których dane dotyczą, i interesy internautów w dostępie do informacji za pośrednictwem dostawców wyszukiwarek internetowych, Trybunał przyjął, że *(c)hoć niewątpliwie chronione na mocy tych postanowień prawa osoby, której dotyczą dane, są również co do zasady nadrzędne wobec tego interesu internautów, to jednak równowaga ta może, w szczególnych przypadkach, zależeć od charakteru rozpatrywanych informacji i od tego, jak istotne są one dla prywatności osoby, której dane dotyczą, oraz dla publicznego interesu w dysponowaniu tą informacją, który to z kolei interes może być uzależniony w szczególności od roli odgrywanej przez tę osobę w życiu publicznym*[13].
48. Trybunał uznał również, że co do zasady prawa osób, których dane dotyczą, będą przewyższały[14] interes internautów w dostępie do informacji za pośrednictwem dostawców wyszukiwarek internetowych. Określił jednak kilka czynników, które mogą mieć wpływ na takie ustalenie. Wśród nich wymienił: charakter informacji lub ich istotność dla prywatności (wrażliwość), a szczególnie interes internautów w dostępie do tych informacji, który to interes może być uzależniony od roli odgrywanej przez tę osobę w życiu publicznym.
49. Z przeprowadzonej przez Trybunał analizy usuwania z listy wyników wyszukiwania wynika, że dokonując oceny żądań usunięcia z listy wyników wyszukiwania, należy koniecznie uwzględnić w decyzji o utrzymaniu lub zablokowaniu wyników wyszukiwania przez dostawcę wyszukiwarki internetowej to jaki byłby wpływ decyzji o usunięciu z listy wyników wyszukiwania na dostęp

[13] TSUE, sprawa C-131/12, wyrok z dnia 13 maja 2014 r., pkt 81; sprawa C-136/17, wyrok z dnia 24 września 2019 r., pkt 66.
[14] TSUE, sprawa C-131/12, wyrok z dnia 13 maja 2014 r., pkt 99; TSUE, sprawa C-136/17, wyrok z dnia 24 września 2019 r., pkt 53.

do informacji dla internautów[15]. Istnienie takiego wpływu nie musi za sobą pociągać odrzucenia żądania usunięcia z listy wyników wyszukiwania. Jak potwierdził Trybunał, taka ingerencja w prawa podstawowe osoby, której dane dotyczą, musi być uzasadniona nadrzędnym interesem szerokiego kręgu odbiorców polegającym na posiadaniu dostępu do danej informacji.

50. Trybunał dokonał również rozróżnienia między legitymacją wydawcy strony internetowej do rozpowszechniania informacji a legitymacją dostawcy wyszukiwarki internetowej. Trybunał stwierdził, że wydawca strony internetowej może podejmować swoją działalność wyłącznie do celów dziennikarskich, w którym to przypadku mógłby korzystać z wyłączeń, które państwa członkowskie mogą ustanowić w takich przypadkach na podstawie art. 9 dyrektywy (obecnie art. 85 ust. 2 RODO). W tym względzie w wyroku *M.L. i W.W. p. Niemcom* z dnia 28 czerwca 2018 r. ETPC wskazuje, że wyważanie wchodzących w grę interesów może prowadzić do różnych wyników w zależności od złożonego wniosku (rozróżniając (i) wniosek o usunięcie złożony w stosunku do podmiotu, który pierwotnie opublikował informację, której działalność zasadniczo jest w centrum tego, co ma chronić wolność wyrażania opinii; (ii) wniosek złożony w stosunku do wyszukiwarki, której głównym interesem nie jest publikacja pierwotnych informacji o osobie, której dane dotyczą, ale ułatwianie identyfikacji wszystkich dostępnych informacji na jej temat i stworzenie jej profilu).
51. Czynniki te należy oceniać względem skarg dotyczących art. 17 RODO, gdyż w decyzjach tych konieczne jest zrównoważenie praw osób, których dane dotyczą, które żądają usunięcia z listy wyników wyszukiwania, z interesami internautów w dostępie do informacji.
52. Jak TSUE wyjaśnił w swoim wyroku w sprawie Google 2, art. 17 ust. 3 lit. a) RODO stanowi *wyraz tego, iż prawo do ochrony danych osobowych nie stanowi prawa bezwzględnego, lecz należy (...) je postrzegać w kontekście jego funkcji społecznej i wyważyć względem innych praw podstawowych w myśl zasady proporcjonalności*[16]. *Wyraźnie ustanawia zatem wymóg zapewnienia równowagi między, z jednej strony, prawami podstawowymi do poszanowania życia prywatnego i ochrony danych osobowych, ustanowionymi w art. 7 i 8 karty, a, z drugiej strony, podstawowym prawem do wolności informacji, zagwarantowanym w art. 11 karty*[17].
53. Trybunał stwierdza, że *w przypadku gdy do operatora wyszukiwarki skierowano żądanie usunięcia linku do strony internetowej, na której są opublikowane dane osobowe należące do szczególnych kategorii danych (...) operator ten musi, na podstawie wszystkich istotnych elementów danego przypadku i uwzględniając powagę ingerencji w ustanowione w art. 7 i 8 karty prawa podstawowe do poszanowania życia prywatnego i ochrony danych osobowych przysługujące osobie, której dane dotyczą, sprawdzić, czy z uwagi na względy związane z ważnym interesem publicznym (...) umieszczenie takiego linku na wyświetlanej liście wyników wyszukiwania mającego za punkt wyjścia imię i nazwisko osoby, której dane dotyczą, jest ściśle niezbędne do ochrony prawa do wolności informacji przysługującego internautom potencjalnie zainteresowanym uzyskaniem, dzięki takiemu wyszukiwaniu, dostępu do tej strony internetowej, która to wolność jest chroniona na podstawie art. 11 karty*[18].
54. Podsumowując, w zależności od okoliczności sprawy dostawcy wyszukiwarek internetowych mogą odmówić usunięcia z listy wyników wyszukiwania treści w przypadku, gdy są w stanie wykazać, że ich ujęcie w wynikach wyszukiwania jest bezwzględnie konieczne do ochrony prawa internautów do wolności informacji.

[15] TSUE, sprawa C-136/17, wyrok z dnia 24 września 2019 r., pkt 56 et seq.
[16] TSUE, sprawa C-136/17, wyrok z dnia 24 września 2019 r., pkt 57.
[17] TSUE, sprawa C-136/17, wyrok z dnia 24 września 2019 r., pkt 59.
[18] TSUE, sprawa C-136/17, wyrok z dnia 24 września 2019 r., pkt 69.

2.2 Przetwarzanie jest niezbędne do wywiązania się z prawnego obowiązku, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi

55. Treść tego wyłączenia sprawia, że trudno je zastosować względem działalności dostawców wyszukiwarek internetowych i może mieć to wpływ na decyzje dotyczące usunięcia z listy wyników wyszukiwania niektórych wyników, gdyż przetwarzanie danych przez dostawców wyszukiwarek internetowych opiera się, co do zasady, na uzasadnionym interesie dostawcy wyszukiwarki internetowej.

2.2.1 Obowiązek prawny

56. Trudno wyobrazić sobie przepisy prawa, które nakładałyby na dostawców wyszukiwarek internetowych obowiązek rozpowszechniania niektórych informacji. Jest to konsekwencją rodzaju prowadzonej przez nich działalności. Dostawcy wyszukiwarek internetowych nie tworzą ani nie przedstawiają informacji.
57. W związku z tym nie wydaje się prawdopodobne, aby przepisy państwa członkowskiego nakładały na dostawców wyszukiwarek internetowych obowiązek publikowania niektórych rodzajów informacji zamiast ustanawiania obowiązku takiej publikacji względem innych stron internetowych, które następnie zostaną powiązane łączem przez dostawcę wyszukiwarki internetowej.
58. Ocenę tę można również rozszerzyć o możliwość, że prawo Unii lub państwa członkowskiego umożliwia organowi publicznemu podejmowanie decyzji, które nakładają na dostawców wyszukiwarek internetowych obowiązek bezpośredniego publikowania informacji, nie zaś poprzez adresy URL do strony internetowej zawierającej dane informacje.
59. Jeżeli istnieją przypadki, w których państwo członkowskie ustanawia obowiązek względem dostawców wyszukiwarek internetowych, zgodnie z którym muszą oni publikować decyzje lub dokumenty zawierające dane osobowe, lub zgodnie z którym organy publiczne są uprawnione do wymagania takiego publikowania, należy zastosować wyłączenie, o którym mowa w art. 17 ust. 3 lit. b) RODO.
60. Zastosowanie takie musi uwzględniać warunki, w jakich jest ustanawiane, a mianowicie to, że przechowywanie informacji, o których mowa, jest konieczne do spełnienia prawnego obowiązku publikacji. Na przykład, że prawny obowiązek lub decyzja organu uprawnionego do jej przyjęcia, może uwzględniać termin publikacji lub jasno wyrażone cele, których osiągnięcie mogło mieć miejsce w określonym przedziale czasowym. W takich przypadkach, jeżeli okaże się, że żądanie usunięcia z listy wyników wyszukiwania przekroczyło wyznaczone terminy, należy uznać, że wyłączenie nie ma już dłużej zastosowania.
61. Przeciwnie, często zdarza się, że w przepisach państwa członkowskiego przewidziano publikację informacji zawierających dane osobowe na stronach internetowych. Nie można uznać obowiązku prawnego publikowania lub przechowywania opublikowanych informacji jako wchodzącego w zakres odstępstwa określonego w art. 17 ust. 3 lit. b) RODO, gdyż nie jest on skierowany do dostawcy wyszukiwarki internetowej, lecz do wydawców stron

internetowych, których treść jest powiązana z indeksem dostawcy wyszukiwarki internetowej. W związku z tym dostawca wyszukiwarki internetowej nie może powołać się na istnienie obowiązku, aby odrzucić żądanie usunięcia z listy wyników wyszukiwania.

62. Ustanawiając równowagę między prawami osób, których dane dotyczą, a interesem internautów w dostępie do informacji, należy jednak uwzględnić prawny obowiązek dotyczący publikowania skierowany do innych wydawców stron internetowych. Fakt, że informacje muszą być publikowane online w ramach zalecenia prawnego lub w następstwie decyzji organu uprawnionego do jej przyjęcia, wskazuje na interes publiczny dostępu do tych informacji.
63. Takie domniemanie istnienia powszechnego interesu publicznego nie działa w taki sam sposób w odniesieniu do stron internetowych, na których zamieszczone są treści, w porównaniu z indeksem wyników dostawcy wyszukiwarki internetowej. Chociaż obowiązek prawny publikowania informacji na pewnej stronie internetowej może prowadzić do wniosku, że informacji tej nie należy usuwać z tej strony, decyzja dotycząca wyników oferowanych przez dostawcę usług wyszukiwania przy przeszukiwaniu zasobów internetowych po wpisaniu w kryteria wyszukiwania głównie imienia i nazwiska może być odmienna.
64. W tych przypadkach przy ocenie żądania usunięcia z listy wyników wyszukiwania nie należy zakładać, że istnienie obowiązku prawnego publikacji nieodłącznie sugeruje, że w zakresie w jakim obowiązek ten jest nałożony na pierwotnych wydawców strony internetowej, nie jest możliwe, aby dostawca wyszukiwarki internetowej zaakceptował usunięcie z listy wyników wyszukiwania.
65. Co do zasady decyzję taką należy podejmować, wyważając prawa osoby, której dane dotyczą, i interesy internautów w dostępie do tych informacji za pośrednictwem dostawcy wyszukiwarki internetowej.

2.2.2 Wykonanie zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej

66. Dostawcy wyszukiwarek internetowych nie są organami publicznymi, nie sprawują zatem sami uprawnień publicznych.
67. Mogliby jednak sprawować takie uprawnienia, jeżeli prawo państwa członkowskiego lub prawo Unii by im je przyznawało. W ten sam sposób mogliby oni pełnić misję interesu publicznego, jeżeli ich działalność byłaby uznawana za niezbędną do wypełnienia interesu publicznego zgodnie z przepisami krajowymi[19].
68. Z uwagi na charakterystyczne cechy dostawców wyszukiwarek internetowych jest mało prawdopodobne, aby państwa członkowskie przyznały im uprawnienia publiczne lub aby uznały ich działalność lub jej część za konieczną do osiągnięcia ustanowionego zgodnie z prawem interesu publicznego.
69. Jeżeli mimo tego zdarzy się przypadek, w którym prawo państw członkowskich przyznaje dostawcom wyszukiwarek internetowych uprawnienia publiczne lub wiąże ich działalność z wypełnianiem interesu publicznego, mogą się oni odwołać do odstępstwa przewidzianego w art. 17 ust. 3 lit. b) RODO. Wcześniejsze rozważania dotyczące przypadków, w których państwo

[19] RODO, art. 6 ust. 3: *Podstawa przetwarzania, o którym mowa w ust. 1 lit. c) i e), musi być określona:*
a) w prawie Unii; lub
b) w prawie państwa członkowskiego, któremu podlega administrator (...).

członkowskie ustanowiło prawny obowiązek przetwarzania informacji przez dostawców wyszukiwarek internetowych mają również znaczenie w tym przypadku.

70. Aby zdecydować o niespełnieniu żądania dotyczącego usunięcia z listy wyników wyszukiwania z powodów związanych z tym wyłączeniem, konieczne jest ustalenie, czy zachowanie informacji w wynikach wyszukiwarki jest niezbędne do realizacji interesu publicznego lub do realizowania pełnomocnictwa.
71. Z drugiej strony prawną definicję uprawnień lub interesu publicznego ustanowiłoby państwo członkowskie, i jeśli dostawca wyszukiwarki internetowej odrzuca żądanie usunięcia z listy wyników wyszukiwania na podstawie tego odstępstwa, należy również rozumieć, że robi to, ponieważ uznaje, że jego działalność jest niezbędna do realizacji interesów publicznych. Dostawca wyszukiwarki internetowej powinien w takim przypadku przedstawić powody, dla których uważa, że prowadzi swoje działanie w interesie publicznym. Bez takiego wyjaśnienia odmowa spełnienia żądania osoby, której dane dotyczą, w sprawie usunięcia z listy wyników wyszukiwania nie może opierać się na odstępstwie.
72. W związku z tym to organ nadzorczy państwa członkowskiego, którego przepisy mają zastosowanie, będzie musiał rozpatrywać ewentualną skargę na podstawie art. 55 ust. 2 RODO.

2.3 Względy interesu publicznego w dziedzinie zdrowia publicznego

73. Wyłączenie to stanowi szczególny przypadek oparty na fakcie, że przetwarzanie jest konieczne dla realizacji interesu publicznego.
74. W tym przypadku interes publiczny ogranicza się do obszaru zdrowia publicznego, lecz, tak jak w przypadku interesu publicznego w każdym innym obszarze, zgodne z prawem podstawy przetwarzania muszą być ustanowione w prawie Unii lub prawie państwa członkowskiego.
75. Z punktu widzenia stosowania tego wyłączenia w kontekście działalności dostawcy wyszukiwarki internetowej można dojść do tych samych wniosków, jak te przedstawione powyżej. Nie wydaje się prawdopodobne, aby prawo państwa członkowskiego lub prawo Unii mogło ustalać stosunek między działalnością dostawcy wyszukiwarki internetowej a przechowywaniem informacji lub kategorii informacji w wynikach wyszukiwania dostawcy wyszukiwarki internetowej, realizując przy tym cele interesu publicznego w dziedzinie zdrowia publicznego.
76. Wniosek taki jest jeszcze bardziej oczywisty, jeżeli wziąć pod uwagę, że skutkiem usunięcia z listy wyników wyszukiwania jest jedynie sytuacja, w której niektóre wyniki są usunięte z wyników wyszukiwania otrzymanych po wpisaniu w kryteria wyszukiwania głównie imienia i nazwiska. Informacje te nie są jednak usuwane z indeksów dostawców wyszukiwarek internetowych i można je pobrać, stosując inne terminy wyszukiwania.
77. Trudno jest zatem wyobrazić sobie, aby przechowywanie takich wyników jako widocznych, gdy przeszukiwanie zasobów internetowych prowadzone po wpisaniu w kryteria wyszukiwania głównie imienia i nazwiska osoby, której dane dotyczą, można było uznać co do zasady jako niezbędne z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego.
78. Powyżej omówiono kryteria stosowania krajowych norm i określanie organu nadzorczego, który jest zobowiązany do rozpatrywania możliwych skarg w przypadkach spraw związanych z art. 17 RODO, które odrzucono, stosując to wyłączenie.

2.4 Do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1, o ile prawdopodobne jest, że prawo, o którym mowa w ust. 1, uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania

79. W takim scenariuszu dostawca wyszukiwarki internetowej musi być w stanie wykazać, że usunięcie pewnych treści z wyników wyszukiwania stanowi poważną przeszkodę lub całkowicie uniemożliwia osiągnięcie celów badań naukowych lub historycznych lub celów statystycznych.
80. Należy rozumieć, że cele te muszą być realizowane w sposób obiektywny przez dostawcę wyszukiwarki internetowej. Prawdopodobieństwo, że usunięcie wyników mogłoby w znaczny sposób wpłynąć na cele badań naukowych lub cele statystyczne realizowane przez użytkowników usługi dostawcy wyszukiwarki internetowej nie jest istotne w odniesieniu do stosowania tego odstępstwa. Cele takie, jeżeli istnieją, należy brać pod uwagę, wyważając prawa osoby, której dane dotyczą, i interesy internautów w dostępie do tych informacji za pośrednictwem dostawcy wyszukiwarki internetowej.
81. Należy również zauważyć, że dostawca wyszukiwarki internetowej może realizować takie cele w sposób obiektywny, bez konieczności powiązania co do zasady między imieniem i nazwiskiem osoby, której dane dotyczą, a wynikami wyszukiwania.

2.5 Ustalanie, dochodzenie lub obrona roszczeń

82. Co do zasady jest wysoce nieprawdopodobne, aby dostawcy wyszukiwarek internetowych mogli wykorzystać to odstępstwo do celu odrzucenia żądania usunięcia z listy wyników wyszukiwania na podstawie art. 17 RODO.
83. Należy dodatkowo podkreślić, że celem żądania usunięcia z listy wyników wyszukiwania jest usunięcie niektórych wyników ze strony wyników wyszukiwania zapewnianych przez dostawcę wyszukiwarki internetowej wskutek przeszukiwania zasobów internetowych prowadzonego po wpisaniu w kryteria wyszukiwania głównie imienia i nazwiska osoby, której dane dotyczą. Informacje są nadal dostępne przy zastosowaniu innych kryteriów wyszukiwania.



Wytyczne nr 4/2019 dotyczące artykułu 25

Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych

Wersja 2.0

Przyjęte 20 października 2020 r.

Historia wersji

Wersja 1.0	13 listopada 2019 r.	Przyjęcie wytycznych do konsultacji publicznych
Wersja 2.0	20 października 2020 r.	Przyjęcie wytycznych przez EROD po konsultacjach publicznych

Spis treści

1 Zakres stosowania 5
2 Analiza art. 25 ust. 1 i ust. 2 Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych 6
2.1 Artykuł 25 ust. 1: Uwzględnianie ochrony danych w fazie projektowania 6
2.1.1 Obowiązek administratora polegający na wdrażaniu odpowiednich środków technicznych i organizacyjnych oraz niezbędnych zabezpieczeń w odniesieniu do przetwarzania 6
2.1.2 Zaprojektowane w celu skutecznej realizacji zasad ochrony danych i ochrony praw i wolności osób, których dane dotyczą 7
2.1.3 Elementy wymagające uwzględnienia 8
2.1.4 Aspekt dotyczący czasu 11
2.2 Artykuł 25 ust. 2: Domyślna ochrona danych 12
2.2.1 Domyślnie przetwarzane są wyłącznie dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania 12
2.2.2 Wymiary obowiązku minimalizacji danych 13
3 Wdrażanie zasad ochrony danych do procesu przetwarzania danych osobowych z wykorzystaniem uwzględniania ochrony danych w fazie projektowania oraz domyślnej ochrony danych 15
3.1 Przejrzystość 16
3.2 Zgodność z prawem 17
3.3 Rzetelność 19
3.4 Ograniczenie celu 21
3.5 Minimalizacja danych 23
3.6 Prawidłowość 25
3.7 Ograniczenie przechowywania 27
3.8 Integralność i poufność 29
3.9 Rozliczalność 31
4 Artykuł 25 ust. 3 – Certyfikacja 31
5 Egzekwowanie przepisów art. 25 i konsekwencje 32
6 Zalecenia 32

Europejska Rada Ochrony Danych

uwzględniając art. 70 ust. 1 lit. e) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (zwanego dalej „RODO"),

uwzględniając Porozumienie EOG, a w szczególności załącznik XI do niego i jego protokół 37, w brzmieniu zmienionym decyzją Wspólnego Komitetu EOG nr 154/2018 z dnia 6 lipca 2018 r.,

uwzględniając art. 12 i 22 swojego regulaminu wewnętrznego,

PRZYJMUJE NINIEJSZE WYTYCZNE:

Streszczenie

W świecie, w którym postępuje proces cyfryzacji, przestrzeganie wymogów ochrony danych w fazie projektowania oraz domyślnej ochrony danych odgrywają niezwykle ważną rolę w promowaniu prywatności i ochrony danych w społeczeństwie. Istotne jest zatem, aby administratorzy poważnie podchodzili do swojej odpowiedzialności i wdrażali zobowiązania wynikające z RODO przy projektowaniu operacji przetwarzania.

Niniejsze wytyczne zawierają ogólne wskazówki dotyczące obowiązku ochrony danych w fazie projektowania oraz domyślnej ochrony danych określonego w art. 25 RODO. Ochrona danych w fazie projektowania oraz domyślna ochrona danych dotyczą wszystkich administratorów danych, niezależnie od wielkości i stopnia złożoności przetwarzania danych. Aby można było wdrożyć wymogi ochrony danych w fazie projektowania oraz domyślnej ochrony danych, administrator danych powinien rozumieć zasady ochrony danych oraz prawa i wolności osoby, której dane dotyczą.

Głównym obowiązkiem jest wdrożenie *odpowiednich* środków i niezbędnych zabezpieczeń, które zapewnią *skuteczną realizację zasad ochrony danych*, a zatem również *praw i wolności osób, których dane dotyczą, już w fazie projektowania oraz jako domyślnej ochrony danych*. W art. 25 określono elementy dotyczące zarówno fazy projektowania, jak i domyślnej ochrony danych, które należy uwzględnić. Elementy te zostaną bardziej szczegółowo omówione w niniejszych wytycznych.

Artykuł 25 ust. 1 stanowi, że administratorzy powinni uwzględnić ochronę danych w fazie projektowania oraz domyślną ochronę danych odpowiednio wcześnie, na etapie planowania kolejnej operacji przetwarzania. Wdrażają oni ochronę danych w fazie projektowania oraz domyślną ochronę danych *przed* przetwarzaniem, a także *w sposób ciągły* podczas przetwarzania, dokonując regularnych przeglądów skuteczności wybranych środków i zabezpieczeń. Ochronę danych w fazie projektowania oraz domyślną ochronę danych stosuje się również do istniejących systemów, które przetwarzają dane osobowe.

Wytyczne zawierają również wskazówki dotyczące sposobów skutecznego wdrażania zasad ochrony danych określonych w art. 5, w ramach których wymieniono kluczowe elementy dotyczące ochrony danych w fazie projektowania i domyślnej ochrony danych, a także przykłady praktycznych rozwiązań. Administrator powinien rozważyć trafność proponowanych środków w kontekście określonego przetwarzania danych, o którym mowa.

EROD przedstawia zalecenia dotyczące sposobu, w jaki administratorzy, podmioty przetwarzające i producenci mogą współpracować w celu realizacji obowiązku ochrony danych w fazie projektowania oraz domyślnej ochrony danych. Zachęca także administratorów z branży, podmioty przetwarzające i producentów, aby stosowali ochronę danych w fazie projektowania oraz domyślną ochronę danych jako metodę, która umożliwi im uzyskanie przewagi konkurencyjnej podczas wprowadzania ich produktów do obrotu względem administratorów i osób, których dane te dotyczą. Nakłania również wszystkich administratorów danych do stosowania certyfikatów i kodeksów postępowania.

1 ZAKRES STOSOWANIA

1. Niniejsze wytyczne dotyczą przede wszystkim wdrażania ochrony danych w fazie projektowania oraz domyślnej ochrony danych przez administratorów zgodnie z obowiązkiem określonym w art. 25 RODO.[1] Inne podmioty, takie jak podmioty przetwarzające oraz wytwórcy produktów, usług i aplikacji (zwani dalej „wytwórcami"), do których art. 25 nie odnosi się bezpośrednio, mogą również uznać niniejsze wytyczne za użyteczne w wytwarzaniu produktów i usług zgodnych z RODO, umożliwiających administratorom wypełnianie ich obowiązków w zakresie ochrony danych.[2] W motywie 78 RODO wprowadzono zapis, że ochronę danych w fazie projektowania oraz domyślną ochronę danych należy uwzględnić w kontekście przetargów publicznych. Mimo że wszyscy administratorzy mają obowiązek włączenia ochrony danych w fazie projektowania oraz domyślnej ochrony danych do swoich czynności przetwarzania, przepis ten wspiera przyjęcie zasad, zgodnie z którymi administracje publiczne powinny dawać przykład. Administrator jest odpowiedzialny za realizację obowiązków w zakresie ochrony danych w fazie projektowania oraz domyślnej ochrony danych z tytułu przetwarzania danych przez jego podmioty przetwarzające i podmioty podprzetwarzające i powinien to uwzględniać przy zawieraniu umów z tymi stronami.

2. Wymóg opisany w art. 25 zobowiązuje administratorów do uwzględnienia zasad ochrony danych już w fazie projektowania i jako domyślnej ochrony; ma to zastosowanie przez cały czas trwania procesu przetwarzania. Wymóg ochrony danych w fazie projektowania oraz domyślnej ochrony danych obejmuje również systemy przetwarzania danych istniejące przed wejściem w życie RODO. Administratorzy są zobowiązani do bieżącej aktualizacji przetwarzania danych zgodnie z RODO. Więcej informacji na temat sposobu utrzymania istniejącego systemu w zgodności z ochroną danych w fazie projektowania oraz domyślną ochroną danych znajduje się w podrozdziale 2.1.4 niniejszych wytycznych. Istotą tego przepisu jest zapewnienie *odpowiedniej* i *skutecznej* ochrony danych, zarówno *w fazie projektowania*, jak i *domyślnej ochrony*, co oznacza, że administratorzy danych powinni być w stanie wykazać, że dysponują odpowiednimi środkami i zabezpieczeniami w zakresie przetwarzania danych, aby zapewnić skuteczność zasad ochrony danych oraz praw i wolności osób, których dane dotyczą.

[1] Przedstawione tu interpretacje mają w równym stopniu zastosowanie do art. 20 dyrektywy (UE) 2016/680 i art. 27 rozporządzenia 2018/1725.

[2] W motywie 78 RODO wyraźnie wskazano tę konieczność: „Jeżeli opracowywane, projektowane, wybierane i użytkowane są aplikacje, usługi i produkty, które opierają się na przetwarzaniu danych osobowych albo przetwarzają dane osobowe w celu realizacji swojego zadania, należy zachęcać wytwórców tych produktów, usług i aplikacji, by podczas opracowywania i projektowania takich produktów, usług i aplikacji wzięli pod uwagę prawo do ochrony danych osobowych i z należytym uwzględnieniem stanu wiedzy technicznej zapewnili administratorom i podmiotom przetwarzającym możliwość wywiązania się ze spoczywających na nich obowiązków ochrony danych".

3. W rozdziale drugim niniejszych wytycznych skoncentrowano się na wykładni wymogów określonych w art. 25 oraz przeanalizowano zobowiązania prawne wprowadzone tym przepisem. W rozdziale trzecim przedstawiono przykłady dotyczące zastosowania ochrony danych w fazie projektowania oraz domyślnej ochrony danych w kontekście szczególnych zasad ochrony danych.

4. W rozdziale czwartym wytycznych omówiono możliwość ustanowienia mechanizmu certyfikacji w celu wykazania zgodności z art. 25, a w rozdziale piątym – sposoby egzekwowania przepisów tego artykułu przez organy nadzorcze. Ponadto wytyczne zawierają zalecenia dla zainteresowanych stron, dotyczące skutecznego wdrażania ochrony danych w fazie projektowania oraz domyślnej ochrony danych. EROD dostrzega trudności, z jakimi borykają się małe i średnie przedsiębiorstwa (zwane dalej „MŚP"), aby w pełni wypełnić obowiązki w zakresie ochrony danych w fazie projektowania oraz domyślnej ochrony danych, i przedstawia dodatkowe zalecenia dla MŚP, które zawarto w rozdziale szóstym.

2 ANALIZA ART. 25 UST. 1 I UST. 2 UWZGLĘDNIANIE OCHRONY DANYCH W FAZIE PROJEKTOWANIA ORAZ DOMYŚLNA OCHRONA DANYCH

5. Celem niniejszego rozdziału jest przeanalizowanie i sformułowanie wytycznych dotyczących wymogów w zakresie ochrony danych w fazie projektowania określonych w art. 25 ust. 1 oraz domyślnej ochrony danych, o której mowa w art. 25 ust. 2. Ochrona danych w fazie projektowania oraz domyślna ochrona danych są pojęciami, które wzajemnie się uzupełniają i wzmacniają. Osoby, których dane dotyczą, odniosą większe korzyści z domyślnej ochrony danych, jeżeli będzie ona realizowana równocześnie z ochroną danych w fazie projektowania – i odwrotnie.

6. Ochrona danych w fazie projektowania oraz domyślna ochrona danych jest wymogiem, któremu podlegają wszyscy administratorzy, łącznie z małymi przedsiębiorstwami i korporacjami wielonarodowymi. W tym przypadku poziom złożoności procesu wdrażania ochrony danych w fazie projektowania oraz domyślnej ochrony danych może zależeć od poszczególnych operacji przetwarzania danych. Niezależnie jednak od ich skali, wprowadzenie ochrony danych w fazie projektowania oraz domyślnej ochrony danych może w każdym przypadku przynieść korzyści administratorom danych i osobom, których dane dotyczą.

2.1 Artykuł 25 ust. 1: Uwzględnianie ochrony danych w fazie projektowania

2.1.1 Obowiązek administratora polegający na wdrażaniu odpowiednich środków technicznych i organizacyjnych oraz niezbędnych zabezpieczeń w odniesieniu do przetwarzania

7. Zgodnie z art. 25 ust. 1 administrator wdraża *odpowiednie* środki techniczne i organizacyjne zaprojektowane w celu realizacji zasad ochrony danych oraz włączenia w proces przetwarzania *niezbędnych zabezpieczeń*, aby spełnić wymogi oraz chronić prawa i wolności osób, których dane dotyczą. Zarówno odpowiednie środki, jak i niezbędne zabezpieczenia, mają służyć temu samemu celowi polegającemu na ochronie praw osób, których dane dotyczą, oraz na zapewnieniu, aby ochrona ich danych osobowych stanowiła część przetwarzania.

8. *Środki techniczne i organizacyjne* oraz niezbędne *zabezpieczenia* mogą być rozumiane w szerokim znaczeniu jako dowolna metoda lub środek, które administrator może zastosować w procesie przetwarzania. Sformułowanie *odpowiednie* oznacza, że środki i niezbędne zabezpieczenia powinny

być dostosowane do osiągnięcia zamierzonego celu, to znaczy, że muszą one *skutecznie* realizować zasady ochrony danych[3]. Wymóg dotyczący odpowiedniości jest zatem ściśle związany z wymogiem dotyczącym skuteczności.

9. Środkiem technicznym lub organizacyjnym oraz zabezpieczeniem może być dowolne działanie, począwszy od zastosowania zaawansowanych rozwiązań technicznych, po podstawowe przeszkolenie pracowników. Przykłady, które mogą okazać się odpowiednie, w zależności od kontekstu i ryzyka związanego z danym przetwarzaniem, obejmują pseudonimizację[4] danych osobowych; przechowywanie danych osobowych dostępnych w ustrukturyzowanym formacie, powszechnie nadającym się do odczytu maszynowego; umożliwienie osobom, których dane dotyczą ingerencji w przetwarzanie; dostarczanie informacji na temat przechowywania danych osobowych; dysponowanie systemami wykrywania złośliwego oprogramowania; szkolenie pracowników w zakresie podstawowej higieny pracy w cyberprzestrzeni; wdrażanie systemów zarządzania prywatnością i bezpieczeństwem informacji, zobowiązujących umownie podmioty przetwarzające do wdrożenia określonych praktyk w zakresie minimalizacji danych itp.

10. Normy, najlepsze praktyki i kodeksy postępowania, honorowane przez stowarzyszenia i inne organy reprezentujące poszczególne kategorie administratorów, mogą być przydatne w ustalaniu odpowiednich środków. Administrator musi jednak sprawdzić, czy środki te są odpowiednie w odniesieniu do przedmiotowego przetwarzania danych.

2.1.2 Zaprojektowane w celu skutecznej realizacji zasad ochrony danych i ochrony praw i wolności osób, których dane dotyczą

11. *Zasady ochrony danych* określono w art. 5 (dalej zwane „zasadami"), *prawa i wolności osób, których dane dotyczą* stanowią podstawowe prawa i wolności osób fizycznych, w szczególności zaś ich prawo do ochrony danych osobowych, których ochrona została określona w art. 1 ust. 2 jako cel RODO (dalej zwane „prawami")[5]. Ich dokładne brzmienie znajduje się w Karcie praw podstawowych Unii Europejskiej. Ważne jest, aby administrator danych rozumiał znaczenie *zasad* i *praw* jako podstawy ochrony udzielanej na podstawie RODO, a zwłaszcza na podstawie obowiązku w zakresie ochrony danych w fazie projektowania oraz domyślnej ochrony danych.

12. W przypadku wdrażania odpowiednich środków technicznych i organizacyjnych, środki i zabezpieczenia powinny być *zaprojektowane* z uwzględnieniem skutecznego wdrożenia każdej z wyżej wymienionych zasad i wynikającej z nich ochrony praw.

Omówienie kwestii skuteczności

13. Skuteczność jest pojęciem leżącym u podstaw uwzględniania ochrony danych w fazie projektowania. Wymóg skutecznego wdrożenia zasad oznacza, że administratorzy muszą wdrożyć niezbędne środki i zabezpieczenia w celu ochrony tych zasad, aby zagwarantować prawa osobom, których dane dotyczą. Każdy wdrożony środek powinien przynieść zamierzone rezultaty w odniesieniu do przetwarzania przewidzianego przez administratora. Spostrzeżenie to ma dwojakie konsekwencje.

14. Po pierwsze, oznacza to, że postanowienia art. 25 nie wymagają wdrożenia określonych środków technicznych i organizacyjnych, ale wskazują, że wybrane środki i zabezpieczenia powinny odnosić się konkretnie do wdrożenia zasad ochrony danych w ramach określonego przetwarzania. Tym samym

[3] Kwestię „skuteczności" omówiono poniżej w podrozdziale 2.1.2.
[4] Zdefiniowana w art. 4 ust. 5 RODO.
[5] Zobacz motyw 4 RODO.

środki i zabezpieczenia należy zaprojektować w taki sposób, aby były solidne, zaś administrator powinien mieć możliwość wdrożenia dodatkowych środków w celu dostosowania ich do potencjalnego wzrostu ryzyka[6]. Skuteczność środków będzie zatem zależeć od kontekstu danego przetwarzania oraz oceny niektórych elementów, które należy wziąć pod uwagę, określając sposoby przetwarzania. Wspomniane wyżej elementy omówiono poniżej w podrozdziale 2.1.3.

15. Po drugie, administratorzy powinni być w stanie wykazać zgodność z obowiązującymi zasadami.

16. Wdrożone środki i zabezpieczenia powinny zapewnić osiągnięcie pożądanego efektu w zakresie ochrony danych, natomiast administrator powinien posiadać dokumentację dotyczącą wdrożonych środków technicznych i organizacyjnych.[7] W tym celu administrator może określić odpowiednie główne wskaźniki skuteczności działania, aby potwierdzić ich skuteczność. Wskaźnik skuteczności działania jest mierzalną wartością wybraną przez administratora danych, która pokazuje, na ile skutecznie osiąga on swój cel w zakresie ochrony danych. Wskaźniki te mogą być *ilościowe*, takie jak odsetek fałszywych wyników pozytywnych lub fałszywych wyników negatywnych, zmniejszenie liczby skarg, skrócenie czasu reakcji, gdy osoby, których dane dotyczą korzystają ze swoich praw; lub *jakościowe*, takie jak oceny działania, stosowanie skali ocen lub oceny ekspertów. Zamiast stosowania wskaźników skuteczności działania administratorzy mogą wykazać, że zasady są skutecznie wdrażane, przedstawiając uzasadnienie oceny skuteczności wybranych środków i zabezpieczeń.

2.1.3 Elementy wymagające uwzględnienia

17. W art. 25 ust. 1 wymieniono elementy, jakie administrator musi uwzględnić przy określaniu środków dotyczących konkretnej operacji przetwarzania. Poniżej przedstawiono wytyczne dotyczące zastosowania tych elementów w fazie projektowania, w tym również projektowania ustawień domyślnych. Wszystkie te elementy pomagają ustalić, czy dany środek jest odpowiedni do skutecznego wdrożenia zasad. Z tego względu każdy z tych elementów nie stanowi celu samego w sobie, ale jest jednym z czynników, które należy uwzględnić łącznie, aby osiągnąć cel.

2.1.3.1 „stan wiedzy technicznej"

18. Pojęcie „stanu wiedzy technicznej" jest obecne w różnych elementach dorobku prawnego UE, np. w dziedzinie ochrony środowiska i bezpieczeństwa produktów. W RODO odniesienie do „stanu wiedzy technicznej"[8] występuje nie tylko w art. 32 w stosunku do środków bezpieczeństwa[9][10], lecz także w art. 25, rozszerzając tym samym zakres odniesienia na wszystkie środki techniczne i organizacyjne uwzględniane przy przetwarzaniu.

19. W kontekście art. 25 odniesienie do „stanu wiedzy technicznej" nakłada na administratorów obowiązek **uwzględnienia obecnego postępu w zakresie technologii** dostępnych na rynku przy określaniu odpowiednich środków technicznych i organizacyjnych. Od administratorów wymaga się więc, aby dysponowali aktualną wiedzą w zakresie postępu technologicznego i na bieżąco śledzili jego rozwój; w jaki sposób technologia może stwarzać ryzyko lub możliwości dla operacji przetwarzania danych; oraz w jaki sposób wdrażać i aktualizować środki i zabezpieczenia służące *bezpiecznej i skutecznej realizacji* zasad i praw osób, których dane dotyczą, biorąc pod uwagę zmieniający się krajobraz technologiczny.

20. „Stan wiedzy technicznej" jest dynamicznym pojęciem, którego nie można definiować statycznie w określonym czasie, ale należy go oceniać *na bieżąco* w kontekście postępu technologicznego. W obliczu postępu technologicznego administrator może stwierdzić, że środek, który kiedyś zapewniał odpowiedni stopień ochrony, już tego nie czyni. Niedbałe zaniedbanie zmian technologicznych może zatem skutkować brakiem zgodności z art. 25.

21. Kryterium „stanu wiedzy technicznej" ma zastosowanie nie tylko do środków technologicznych, ale również do środków organizacyjnych. Brak odpowiednich środków organizacyjnych może przyczynić się do obniżenia, a nawet do całkowitego podważenia skuteczności wybranej technologii. Przykładem środków organizacyjnych może być wdrożenie polityki wewnętrznej, szkolenia w zakresie technologii, bezpieczeństwa i ochrony danych oraz strategie bezpieczeństwa technologii informacyjnych i zarządzanie nimi.

22. Istniejące i uznane ramy, standardy, certyfikaty, kodeksy postępowania itp. w różnych dziedzinach mogą mieć znaczenie dla wskazania aktualnego „stanu wiedzy technicznej" w ramach danego obszaru zastosowania. Jeśli normy takie istnieją i zapewniają wysoki stopień ochrony osoby, której dane dotyczą, zgodnie z wymogami prawnymi lub wykraczając poza te wymogi, administratorzy powinni je uwzględniać w fazie projektowania i wdrażania środków ochrony danych.

2.1.3.2 „koszt wdrażania"

23. Administrator może wziąć pod uwagę koszt wdrożenia, wybierając i stosując odpowiednie środki techniczne i organizacyjne oraz niezbędne zabezpieczenia, które zapewniają skuteczną realizację zasad w celu ochrony praw osób, których dane dotyczą. Koszt odnosi się do zasobów ogółem, w tym do czasu i zasobów ludzkich.

24. Element ten nie wiąże się z koniecznością wydatkowania przez administratora nieproporcjonalnie dużych zasobów, jeśli istnieją inne, bardziej ekonomiczne i wciąż skuteczne środki. Koszt wdrożenia jest jednak czynnikiem, który należy uwzględnić przy wdrożeniu ochrony danych w fazie projektowania, nie zaś podstawą do odstąpienia od tego wdrożenia.

25. Wybrane środki muszą więc zapewniać, aby czynność przetwarzania danych przewidziana przez administratora nie odbywała się z naruszeniem zasad, niezależnie od kosztów. Administratorzy powinni być w stanie zarządzać ogólnymi kosztami, aby mogli skutecznie wdrażać wszystkie zasady i, w konsekwencji, chronić prawa.

[6] „Podstawowe zasady obowiązujące administratorów (tj. zasada zgodności z prawem, minimalizacji danych, ograniczenia celu, przejrzystości, integralności danych, prawidłowości danych) powinny pozostać bez zmian, niezależnie od przetwarzania i ryzyka dla osób, których dane dotyczą. Należyte uwzględnienie charakteru i zakresu takiego przetwarzania zawsze było jednak integralną częścią stosowania tych zasad, aby były z natury skalowalne". Grupa Robocza Art. 29. „Stanowisko w sprawie podejścia opartego na ryzyku w ramach prawnych ochrony danych". WP 218, 30 maja 2014 r., s. 3. ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf

[7] Zob. motywy 74 i 78.

[8] Zobacz decyzja niemieckiego Federalnego Trybunału Konstytucyjnego w sprawie „Kalkar" z 1978 r.: https://germanlawarchive.iuscomp.org/?p=67, która może stanowić podstawę metodyki obiektywnej definicji pojęcia. Na tej podstawie poziom „stanu wiedzy technicznej" będzie określany w przedziale między poziomem technologicznym „istniejącej wiedzy naukowej i istniejących badań naukowych" a bardziej ugruntowanymi „ogólnie przyjętymi zasadami technologii". „Stan wiedzy technicznej" można zatem określić jako poziom technologiczny usługi lub technologii lub produktu, który istnieje na rynku i jest najbardziej skuteczny w osiąganiu wyznaczonych celów.

[9] https://www.enisa.europa.eu/news/enisa-news/what-is-state-of-the-art-in-it-security

[10] www.teletrust.de/en/publikationen/broschueren/state-of-the-art-in-it-security/

2.1.3.3 „charakter, zakres, kontekst i cele przetwarzania"

26. Ustalając niezbędne środki, administratorzy muszą brać pod uwagę charakter, zakres, kontekst i cel przetwarzania danych.

27. Czynniki te należy interpretować zgodnie z rolą, jaką pełnią one w innych przepisach RODO, jak na przykład w art. 24, 32 i 35, aby zaprojektować zasady ochrony danych jako część procesu ich przetwarzania.

28. W skrócie, pojęcie **charakteru** można rozumieć jako nieodłączną[11] cechę przetwarzania. **Zakres** odnosi się do wielkości i zasięgu przetwarzania. **Kontekst** związany jest z okolicznościami przetwarzania, które mogą wpływać na oczekiwania osoby, której dane dotyczą, natomiast **cel** odnosi się do celów przetwarzania.

2.1.3.4 „ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania"

29. W wielu przepisach zawartych w art. 24, 25, 32 i 35 RODO przyjęto spójne podejście oparte na ryzyku, aby określić odpowiednie środki techniczne i organizacyjne służące ochronie osób fizycznych, ich danych osobowych oraz zapewnieniu zgodności z wymogami RODO. Aktywa podlegające ochronie są zawsze takie same (osoby fizyczne, przez ochronę ich danych osobowych), są chronione przed takimi samymi zagrożeniami (w odniesieniu do praw i wolności osób fizycznych), z uwzględnieniem tych samych warunków (charakteru, zakresu, kontekstu i celów przetwarzania).

30. Przeprowadzając analizę ryzyka pod kątem zgodności z art. 25, administrator musi określić zagrożenia dla praw osób, których dane dotyczą, jakie stanowi naruszenie zasad, oraz określić prawdopodobieństwo i wagę tych zagrożeń w celu wdrożenia środków służących skutecznemu ich zminimalizowaniu. Systematyczna i gruntowna ocena przetwarzania danych ma kluczowe znaczenie przy dokonywaniu oceny ryzyka. Administrator ocenia na przykład szczególne zagrożenia związane z brakiem dobrowolnie wyrażonej zgody, stanowiącym naruszenie zasady zgodności z prawem, podczas przetwarzania danych osobowych dzieci i młodzieży poniżej 18. roku życia jako grupy szczególnie narażonej, w przypadku gdy nie ma innej podstawy prawnej, i wdraża odpowiednie środki w celu ograniczenia i skutecznego zminimalizowania zidentyfikowanych zagrożeń związanych z tą grupą osób, których dane dotyczą.

31. W „Wytycznych EROD dotyczących oceny skutków dla ochrony danych (DPIA)"[12], w których skoncentrowano się na określeniu, czy operacja przetwarzania może prowadzić do wysokiego ryzyka, przedstawiono również wskazówki dotyczące sposobu oceny ryzyka związanego z ochroną danych oraz sposobu przeprowadzania oceny ryzyka związanego z ochroną danych. Wytyczne te mogą być również przydatne podczas oceny ryzyka w odniesieniu do wszystkich wspomnianych wyżej artykułów, w tym art. 25.

[11] Przykładami są szczególne kategorie danych osobowych, automatyczne podejmowanie decyzji, wypaczone relacje władzy, nieprzewidywalne przetwarzanie, utrudnienia związane z korzystaniem z praw przez osobę, której dane dotyczą itp.

[12] Grupa Robocza Art. 29 „Wytyczne dotyczące oceny skutków dla ochrony danych (DPIA) oraz ustalenia, czy przetwarzanie »z dużym prawdopodobieństwem może powodować wysokie ryzyko«, do celów rozporządzenia 2016/679". WP 248 rev.01, 4 października 2017 r. ec.europa.eu/newsroom/document.cfm?doc_id=47711 – zatwierdzone przez EROD.

32. Podejście oparte na ryzyku nie wyklucza stosowania punktów odniesienia, najlepszych praktyk ani norm. Elementy te mogą stanowić przydatny zestaw narzędzi dla administratorów służący przeciwdziałaniu podobnemu ryzyku w podobnych sytuacjach (charakter, zakres, kontekst i cele przetwarzania). Obowiązek określony w art. 25 (a także w art. 24, 32 i art. 35 ust. 7 lit. c) RODO) polegający na uwzględnieniu „ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikającego z przetwarzania" pozostaje jednak bez zmian. W związku z tym administratorzy, mimo że korzystają z takich narzędzi, muszą zawsze przeprowadzić indywidualną ocenę ryzyka w zakresie ochrony danych w odniesieniu do danej czynności przetwarzania danych oraz sprawdzić skuteczność odpowiednich środków i proponowanych zabezpieczeń. Dodatkowo wymagana może być wówczas ocena skutków dla ochrony danych lub aktualizacja istniejącej oceny skutków dla ochrony danych.

2.1.4 Aspekt dotyczący czasu

2.1.4.1 Przy określaniu sposobów przetwarzania

33. Uwzględnianie ochrony danych w fazie projektowania należy wdrażać *„przy określaniu sposobów przetwarzania"*.

34. Zakres „sposobów przetwarzania" obejmuje elementy projektowe przetwarzania, od ogólnych po szczegółowe, w tym architektura, procedury, protokoły, układ i wygląd.

35. „Czas określania sposobów przetwarzania" odnosi się do okresu, w którym administrator podejmuje decyzję o sposobie, w jaki przetwarzanie będzie prowadzone, oraz o sposobie, w jaki będzie ono przebiegać, a także w kwestii mechanizmów, które zostaną użyte do realizacji takiego przetwarzania. Podczas podejmowania takich decyzji administrator musi ocenić odpowiednie środki i zabezpieczenia w celu skutecznego wdrażania zasad i praw osób, których dane dotyczą, do procesu przetwarzania oraz musi uwzględnić elementy takie jak stan wiedzy technicznej, koszt wdrażania, charakter, zakres, kontekst i cel oraz ryzyko. Należy do nich również czas pozyskania i wdrożenia oprogramowania, sprzętu i usług do przetwarzania danych.

36. Wczesne uwzględnienie ochrony danych w fazie projektowania oraz domyślnej ochrony danych ma kluczowe znaczenie dla pomyślnego wdrożenia zasad i ochrony praw osób, których dane dotyczą. Ponadto, z perspektywy stosunku kosztów do korzyści, w interesie administratora leży szybsze uwzględnienie tej kwestii, ponieważ wprowadzanie zmian do istniejących już planów i zaprojektowanych już operacji przetwarzania mogłoby być trudne i kosztowne.

2.1.4.2 Podczas procesu przetwarzania (utrzymanie i przegląd wymogów w zakresie ochrony danych)

37. Po rozpoczęciu procesu przetwarzania administrator ma stały obowiązek utrzymania ochrony danych w fazie projektowania oraz domyślnej ochrony danych, tj. dalszego skutecznego wdrażania zasad w celu ochrony praw, śledzenia aktualnego stanu wiedzy technicznej, ponownej oceny poziomu ryzyka itd. Charakter, zakres i kontekst operacji przetwarzania, a także ryzyko mogą się zmieniać w toku przetwarzania, co oznacza, że administrator danych musi dokonać ponownej oceny operacji przetwarzania prowadząc regularne przeglądy i oceny skuteczności wybranych środków i zabezpieczeń.

38. Obowiązek utrzymania, przeglądu i aktualizacji, w miarę potrzeby, operacji przetwarzania dotyczy również wcześniej istniejących systemów. Oznacza to, że dotychczasowe systemy zaprojektowane przed wejściem w życie RODO należy poddawać przeglądom i konserwacji, aby zapewnić wdrożenie

środków i zabezpieczeń, które w skuteczny sposób wdrażają zasady i prawa osób, których dane dotyczą, jak określono w niniejszych wytycznych.

39. Zakres tego obowiązku obejmuje również wszelkie procesy przetwarzania prowadzone przez podmioty przetwarzające dane. Operacje podmiotów przetwarzających powinny być poddawane regularnym przeglądom i ocenom przez administratorów w celu zapewnienia, że umożliwiają one stałą zgodność z zasadami i pozwalają administratorowi danych na wykonywanie jego obowiązków w tym zakresie.

2.2 Artykuł 25 ust. 2: Domyślna ochrona danych

2.2.1 Domyślnie przetwarzane są wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania

40. „Wartość domyślna", zgodnie z definicją powszechnie stosowaną w dziedzinie informatyki, odnosi się do istniejącej wcześniej lub wstępnie wybranej wartości konfigurowalnego ustawienia przypisanego do oprogramowania użytkowego (aplikacji), programu komputerowego lub urządzenia. Ustawienia takie nazywane są również „ustawieniami domyślnymi" lub „ustawieniami fabrycznymi", szczególnie w przypadku urządzeń elektronicznych.

41. Dlatego też termin „domyślne" w przypadku przetwarzania danych osobowych odnosi się do podejmowania decyzji dotyczących wartości konfiguracyjnych lub opcji przetwarzania, które są ustawione lub zapisane w systemie przetwarzania, takim jak: aplikacja, usługa lub urządzenie, lub też ręczna procedura przetwarzania, mających wpływ na ilość gromadzonych danych osobowych, zakres ich przetwarzania, okres ich przechowywania i ich dostępność.

42. Administrator powinien wybrać i odpowiadać za wdrożenie domyślnych ustawień ochrony danych i opcji w taki sposób, aby jedynie przetwarzanie, które jest ściśle niezbędne do osiągnięcia określonego, zgodnego z prawem celu, było realizowane domyślnie. W takim przypadku administratorzy muszą polegać na swojej ocenie konieczności (niezbędności) przetwarzania w odniesieniu do podstaw prawnych art. 6 ust. 1. Oznacza to, że domyślnie administrator danych nie gromadzi większej liczby danych niż jest to niezbędne, nie przetwarza zgromadzonych danych w zakresie większym niż jest to niezbędne do realizacji celów, ani nie przechowuje danych dłużej niż jest to niezbędne. Podstawowy wymóg zakłada, że ochrona danych jest domyślnie wbudowana w ich przetwarzanie.

43. Administrator jest zobowiązany wstępnie określić konkretne, wyraźne i prawnie uzasadnione cele gromadzenia i przetwarzania danych osobowych[13].Środki muszą być w sposób domyślny odpowiednie, aby zapewnić przetwarzanie wyłącznie tych danych osobowych, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. „Wytyczne dotyczące oceny konieczności i proporcjonalności środków ograniczających prawo do ochrony danych osobowych" przygotowane przez EIOD mogą być również użyteczne przy podejmowaniu decyzji dotyczących tego, które dane są niezbędne do przetworzenia, aby osiągnąć konkretny cel[14] [15] [16].

44. Jeżeli administrator korzysta z oprogramowania osób trzecich lub oprogramowania dostępnego na rynku, powinien przeprowadzić ocenę ryzyka związanego z produktem i upewnić się, że jego funkcje, które nie mają podstawy prawnej lub nie są zgodne z zamierzonymi celami przetwarzania, zostaną wyłączone.

45. Te same względy mają zastosowanie do środków organizacyjnych wspierających operacje przetwarzania. Należy je zaprojektować tak, aby na początku przetwarzać jedynie minimalną ilość danych osobowych, niezbędną do realizacji konkretnych operacji. Trzeba to szczególnie uwzględnić przy udzielaniu dostępu do danych pracownikom o różnych rolach i odmiennych potrzebach w zakresie dostępu.

46. Odpowiednie „środki techniczne i organizacyjne" w kontekście domyślnej ochrony danych są rozumiane w taki sam sposób, jak omówiono powyżej w sekcji 2.1.1, ale mają zastosowanie szczególnie do zasady minimalizacji danych.

47. Wspomniany wcześniej obowiązek polegający na przetwarzaniu wyłącznie tych danych osobowych, które są niezbędne dla osiągnięcia każdego konkretnego celu, ma zastosowanie do następujących elementów:

2.2.2 Wymiary obowiązku minimalizacji danych

48. W art. 25 ust. 2 wyszczególniono wymiary obowiązku minimalizacji danych w przypadku przetwarzania domyślnego, określając przy tym, że obowiązek ten ma zastosowanie do ilości gromadzonych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności.

2.2.2.1 „ilości zbieranych danych osobowych"

49. Administratorzy muszą uwzględnić zarówno ilość danych osobowych, jak i rodzaje, kategorie i poziom szczegółowości danych osobowych wymagane do celów przetwarzania. Dokonując wyborów w zakresie projektowania, powinni oni uwzględnić zwiększone ryzyko dla zasad integralności i poufności, minimalizacji danych i ograniczenia ich przechowywania podczas gromadzenia dużych ilości szczegółowych danych osobowych oraz porównać je z ograniczeniem ryzyka podczas gromadzenia mniejszych ilości lub mniej szczegółowych informacji na temat osób, których dane dotyczą. W żadnym przypadku domyślne ustawienia nie mogą obejmować zbierania danych osobowych, które nie są niezbędne do osiągnięcia konkretnego celu przetwarzania. Innymi słowy, jeżeli określone kategorie danych osobowych są zbędne lub jeżeli szczegółowe dane nie są potrzebne, ponieważ mniej szczegółowe dane są wystarczające, nie można gromadzić żadnych nadwyżek danych osobowych.

[13] Artykuł 5 ust. 1 lit. b), c), d), e) RODO.

[14] EIOD. „Wytyczne dotyczące oceny konieczności i proporcjonalności środków ograniczających prawo do ochrony danych". 25 lutego 2019 r. https://edps.europa.eu/sites/edp/files/publication/19-02-25_proportionality_guidelines_en.pdf

[15] Zob. również EIOD. „Ocena konieczności wprowadzenia środków ograniczających podstawowe prawo do ochrony danych osobowych: zestaw narzędzi" https://edps.europa.eu/data-protection/our-work/publications/papers/necessity-toolkit_en

[16] Więcej informacji na temat konieczności, zob. Grupa Robocza Art. 29. „Opinia 06/2014 w sprawie pojęcia uzasadnionych interesów administratora danych zawartego w art. 7 dyrektywy 95/46/WE". WP 217, 9 kwietnia 2014 r. ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf

50. Te same domyślne wymogi mają zastosowanie do usług niezależnie od tego, jakiej platformy lub jakiego urządzenia użyto. W tym kontekście można gromadzić jedynie dane osobowe niezbędne do realizacji danego celu.

2.2.2.2 „zakresu ich przetwarzania"

51. Operacje przetwarzania[17] przeprowadzane na danych osobowych nie wykraczają poza to, co niezbędne. Wiele operacji przetwarzania może przyczynić się do osiągnięcia celu przetwarzania. Fakt, że pewne dane osobowe są niezbędne do realizacji celu, nie oznacza jednak, że na danych mogą być wykonywane operacje przetwarzania każdego rodzaju i o dowolnej częstotliwości. Administratorzy powinni również uważać, by nie rozszerzać granic „zgodnych celów" określonych w art. 6 ust. 4 i mieć na uwadze taki zakres przetwarzania, który będzie zgodny z uzasadnionymi oczekiwaniami osób, których dane dotyczą.

2.2.2.3 „okresu ich przechowywania"

52. Zgromadzonych danych osobowych nie przechowuje się, jeżeli nie jest to niezbędne do celów ich przetwarzania oraz jeżeli nie istnieje inny zgodny cel i podstawa prawna zgodnie z art. 6 ust. 4. Każde zatrzymywanie danych powinno być w razie potrzeby obiektywnie uzasadnione przez administratora danych zgodnie z zasadą rozliczalności.

53. Administrator danych powinien ograniczyć okres zatrzymywania do niezbędnego minimum dla osiągnięcia danego celu. Jeżeli dane osobowe nie są już niezbędne do celów przetwarzania, są one domyślnie usuwane lub anonimizowane. Długość okresu zatrzymywania danych będzie zatem uzależniona od celu przetwarzania, o którym mowa. Obowiązek ten bezpośrednio wynika z zasady ograniczenia przechowywania, o której mowa w art. 5 ust. 1 lit. e), i jest realizowany w ramach domyślnej ochrony danych, tj. administrator danych powinien posiadać stałe procedury usuwania lub anonimizacji danych stanowiące cześć przetwarzania.

54. Anonimizacja[18] danych osobowych jest alternatywą dla ich usuwania, pod warunkiem że uwzględniono wszystkie odpowiednie elementy kontekstowe, a prawdopodobieństwo wystąpienia ryzyka i jego powaga, w tym ryzyko związane z ponowną identyfikacją, są regularnie oceniane[19].

2.2.2.4 „ich dostępności"

55. Administrator powinien wprowadzić ograniczenia dotyczące dostępu do danych osobowych oraz rodzaju tego dostępu na podstawie oceny konieczności, a także sprawdzić, czy dane osobowe są rzeczywiście dostępne dla podmiotów, którym są one potrzebne w razie potrzeby, na przykład w sytuacjach nadzwyczajnych. Kontroli dostępu należy przestrzegać podczas całego przepływu danych w ramach przetwarzania.

[17] Zgodnie z art. 4 ust. 2 RODO obejmują one zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.
[18] Grupa Robocza Art. 29: „Opinia 05/2014 w sprawie technik anonimizacji". WP 216, 10 kwietnia 2014 r. ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf
[19] Zobacz art. 4 ust. 1 RODO, motyw 26 RODO, Grupa Robocza Art. 29 „Opinia 05/2014 w sprawie technik anonimizacji". Zobacz również podsekcję „Ograniczenie przechowywania" w sekcji 3 niniejszego dokumentu, odnoszącą się do konieczności zapewnienia przez administratora skuteczności wdrożonych technik anonimizacji.

56. W art. 25 ust. 2 stwierdzono ponadto, że dane osobowe nie mogą być udostępniane nieokreślonej liczbie osób fizycznych bez interwencji danej osoby. Administrator domyślnie ogranicza dostępność danych i zapewnia osobie, której dane dotyczą, możliwość podjęcia interwencji przed opublikowaniem lub udostępnieniem w inny sposób jej danych osobowych w odniesieniu do nieokreślonej liczby osób fizycznych.

57. Udostępnienie danych osobowych nieokreślonej liczbie osób może skutkować dalszym rozpowszechnianiem danych niż to pierwotnie zamierzono. Jest to szczególnie istotne w kontekście Internetu i wyszukiwarek internetowych. W związku z tym administratorzy powinni w ramach domyślnej ochrony danych umożliwić osobom, których dane dotyczą, podjęcie odpowiednich działań przed udostępnieniem ich danych osobowych w otwartym Internecie. Ma to szczególne znaczenie w przypadku dzieci i grup szczególnie wrażliwych.

58. W zależności od podstawy prawnej przetwarzania, możliwość podjęcia interwencji może zmieniać się stosownie do kontekstu przetwarzania. Przykładem może być prośba o zgodę na powszechne udostępnienie danych osobowych lub o wprowadzenie ustawień prywatności, aby osoby, których dane dotyczą, mogły same kontrolować publiczny dostęp do nich.

59. Nawet jeżeli dane osobowe są udostępniane za zgodą i wiedzą osoby, której dane dotyczą, nie oznacza to, że każdy inny administrator posiadający dostęp do tych danych osobowych może je swobodnie przetwarzać do własnych celów – musi dysponować odrębną podstawą prawną[20].

3 WDRAŻANIE ZASAD OCHRONY DANYCH DO PROCESU PRZETWARZANIA DANYCH OSOBOWYCH Z WYKORZYSTANIEM UWZGLĘDNIANIA OCHRONY DANYCH W FAZIE PROJEKTOWANIA ORAZ DOMYŚLNEJ OCHRONY DANYCH

60. Na każdym etapie projektowania czynności przetwarzania, w tym zakupów, przetargów, outsourcingu, rozwoju, wsparcia, utrzymania, testowania, przechowywania, usuwania itp., administrator powinien wziąć pod uwagę i przeanalizować różne elementy ochrony danych w fazie projektowania oraz domyślnej ochrony danych, które zostaną zilustrowane przykładami w tym rozdziale w kontekście wdrażania zasad[21] [22] [23].

61. Administratorzy muszą wdrożyć zasady umożliwiające realizację ochrony danych w fazie projektowania oraz domyślnej ochrony danych. Zasady te obejmują: przejrzystość, zgodność z prawem, rzetelność, ograniczenie celu, minimalizację danych, prawidłowość, ograniczenie przechowywania, integralność i poufność oraz rozliczalność. Zasady te są przedstawione w art. 5 i w motywie 39 RODO. Aby w pełni zrozumieć sposób wdrażania ochrony danych w fazie projektowania oraz domyślnej ochrony danych, ważne jest zrozumienie znaczenia każdej z tych zasad.

[20] Zobacz sprawa Satakunnan Markkinapörssi Oy i Satamedia Oy przeciwko Finlandii, nr 931/13.
[21] Więcej przykładów znajduje się w wytycznych norweskiego organu ochrony danych: „Tworzenie oprogramowania z uwzględnieniem ochrony danych w fazie projektowania oraz domyślnej ochrony danych". 28 listopada 2017 r. www.datatilsynet.no/en/about-privacy/virksomhetenes-plikter/innebygd-personvern/data-protection-by-design-and-by-default/?id=7729
[22] https://www.cnil.fr/en/cnil-publishes-gdpr-guide-developers
[23] https://www.aepd.es/sites/default/files/2019-12/guia-privacidad-desde-diseno_en.pdf

62. Prezentując przykłady dotyczące sposobu nadania wymiaru operacyjnego ochrony danych w fazie projektowania oraz domyślnej ochrony danych, sporządziliśmy wykazy **kluczowych elementów ochrony danych w fazie projektowania oraz domyślnej ochrony danych** w odniesieniu do każdej z zasad. Chociaż przedstawione przykłady podkreślają przedmiotową szczególną zasadę ochrony danych, mogą również pokrywać się z innymi ściśle powiązanymi zasadami. EROD podkreśla, że przedstawione poniżej kluczowe elementy i przykłady nie są wyczerpujące ani wiążące, lecz mają stanowić jedynie wytyczne dla każdej z zasad. Administratorzy powinni ocenić, w jaki sposób należy zagwarantować zgodność z zasadami w kontekście rozpatrywanej, konkretnej operacji przetwarzania.

63. Niniejsza część dotyczy wprawdzie wdrażania zasad, jednak administrator danych powinien też wprowadzić *odpowiednie* i *skuteczne* sposoby ochrony praw osób, których dane dotyczą, również zgodnie z rozdziałem III RODO, o ile nie wynika to już z samych zasad.

64. Nadrzędna jest tu zasada rozliczalności, która nakłada na administratora odpowiedzialność za wybór niezbędnych środków technicznych i organizacyjnych.

3.1 Przejrzystość[24]

65. Administrator musi zachować jasność i otwartość wobec osoby, której dane dotyczą, w kwestii sposobu, w jaki będzie gromadził, wykorzystywał i udostępniał jej dane osobowe. Przejrzystość polega na umożliwieniu osobom, których dane dotyczą, zrozumienia i – w razie konieczności – skorzystania z ich praw określonych w art. 15–22. Zasada ta jest zawarta w art. 12, 13, 14 i 34. Środki i zabezpieczenia wdrożone w celu wspierania zasady przejrzystości powinny również wspierać wykonanie przepisów tych artykułów.

66. Kluczowe elementy uwzględniania ochrony danych w fazie projektowania i domyślnej ochrony danych w stosunku do zasady przejrzystości mogą obejmować:

- jasność – informacje są podawane jasnym i prostym językiem, są zwięzłe i zrozumiałe;
- semantykę – komunikacja ma jasne znaczenie dla danej grupy odbiorców;
- dostępność – informacje są łatwo dostępne dla osoby, której dane dotyczą;
- kontekst – informacje są przekazywane w odpowiednim czasie i w odpowiedniej formie;
- stosowność – informacje są stosowne i mają zastosowanie do konkretnej osoby, której dane dotyczą;
- uniwersalny projekt – informacje są dostępne dla wszystkich osób, których dotyczą dane, łącznie z wykorzystaniem języków odczytu maszynowego w celu ułatwienia i zautomatyzowania czytelności i przejrzystości;
- zrozumiałość – osoby, których dane dotyczą, muszą dokładnie rozumieć, czego mogą oczekiwać w odniesieniu do przetwarzania ich danych osobowych, szczególnie w przypadku, gdy osobami, których dane dotyczą, są dzieci lub członkowie innych grup szczególnie wrażliwych;
- wielokanałowość – informacje powinny być przekazywane za pośrednictwem różnych kanałów i mediów, nie tylko w formie tekstowej, w celu zwiększenia prawdopodobieństwa skutecznego dotarcia informacji do osoby, której dane dotyczą.
- warstwowość – informacje powinny być ułożone warstwowo w sposób, który rozwiązuje problem napięcia między kompletnością a zrozumieniem, przy jednoczesnym uwzględnieniu uzasadnionych oczekiwań osób, których dane dotyczą.

[24] Opracowanie dotyczące sposobu zrozumienia koncepcji przejrzystości znajduje się w wytycznych Grupy Roboczej Art. 29: „Wytyczne dotyczące przejrzystości na mocy rozporządzenia 2016/679". WP 260 rev.01, 11 kwietnia 2018 r. https://uodo.gov.pl/pl/file/1430 – zatwierdzone przez EROD.

Przykład[25]

Administrator danych projektuje politykę prywatności na swojej stronie internetowej w celu spełnienia wymogów przejrzystości. Polityka prywatności nie powinna zawierać obszernej masy informacji, które są trudne do przeniknięcia i zrozumienia dla przeciętnej osoby, której dane dotyczą. Powinna ona być sformułowana w jasnym i zwięzłym języku oraz umożliwiać użytkownikowi strony internetowej zrozumienie, w jaki sposób przetwarzane są jego dane osobowe. W związku z tym administrator dostarcza informacji w sposób wielowarstwowy, podkreślając najważniejsze punkty. Szczegółowe informacje są łatwo dostępne. Rozwijane menu i linki do innych stron służą dalszemu wyjaśnieniu różnych pozycji i pojęć zawartych w polityce. Administrator zapewnia również, aby informacje były przekazywane w sposób wielokanałowy, dostarczając filmy wideo w celu wyjaśnienia najważniejszych punktów informacji. Synergia pomiędzy poszczególnymi stronami jest niezbędna, aby zapewnić, że podejście warstwowe nie zwiększa dezorientacji, a raczej ją ogranicza.

Dostęp do polityki prywatności nie powinien być utrudniony dla osób, których dane dotyczą. Polityka prywatności jest zatem dostępna i widoczna na wszystkich wewnętrznych stronach WWW danej strony, tak aby osobę, której dane dotyczą, od uzyskania informacji dzieliło tylko jedno kliknięcie. Dostarczane informacje są również projektowane zgodnie z najlepszymi praktykami i standardami uniwersalnego projektowania, tak aby były dostępne dla wszystkich.

Ponadto niezbędne informacje muszą być również dostarczane we właściwym kontekście i w odpowiednim czasie. Ze względu na fakt, że administrator danych przeprowadza wiele operacji przetwarzania danych z wykorzystaniem danych zgromadzonych na stronie internetowej, ogólna polityka prywatności zawarta na stronie internetowej nie wystarczy, aby spełnić wymogi przejrzystości. Administrator projektuje zatem przepływ informacji, przedstawiając osobie, której dane dotyczą, istotne informacje w odpowiednim kontekście, wykorzystując np. fragmenty informacji lub wyskakujące okienka. Na przykład, prosząc osobę, której dane dotyczą, o wprowadzenie danych osobowych, administrator informuje tę osobę o sposobie, w jaki będą przetwarzane jej dane osobowe, oraz dlaczego przetwarzanie tych danych osobowych jest niezbędne.

3.2 Zgodność z prawem

67. Administrator określa ważną podstawę prawną przetwarzania danych osobowych. Środki i zabezpieczenia powinny wspierać wymóg dotyczący zagwarantowania, że cały proces przetwarzania danych jest zgodny z odpowiednimi podstawami prawnymi przetwarzania.

68. Kluczowe elementy uwzględniania ochrony danych w fazie projektowania i domyślnej ochrony danych w stosunku do zgodności z prawem mogą obejmować:

- stosowność – właściwe podstawy prawne mają zastosowanie do przetwarzania;
- zróżnicowanie[26] – podstawa prawna stosowana w odniesieniu do każdej czynności przetwarzania jest zróżnicowana;

[25] Francuski organ ochrony danych opublikował szereg przykładów przedstawiających najlepsze praktyki w zakresie informowania użytkowników oraz innych zasad przejrzystości: https://design.cnil.fr/en/.
[26] EROD. „Wytyczne 2/2019 w sprawie przetwarzania danych osobowych zgodnie z art. 6 ust. 1 lit. b) RODO w kontekście świadczenia usług online osobom, których dane dotyczą". Wersja 2.0, 8 października 2019 r. edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf

- konkretny cel – właściwa podstawa prawna musi być wyraźnie powiązana z konkretnym celem przetwarzania[27];
- konieczność (niezbędność) – przetwarzanie musi być niezbędne i bezwarunkowe, aby jego cel był zgodny z prawem;
- autonomię – osobie, której dane dotyczą, należy przyznać najwyższy możliwy stopień autonomii w odniesieniu do kontroli nad danymi osobowymi w ramach podstawy prawnej;
- uzyskanie zgody – zgoda musi być dobrowolna, konkretna, świadoma i jednoznaczna[28]. Szczególną uwagę należy zwrócić na zdolność dzieci i młodzieży do wyrażenia świadomej zgody;
- wycofanie zgody – w przypadku gdy podstawą prawną jest zgoda, przetwarzanie danych powinno ułatwiać wycofanie zgody. Wycofanie musi być równie proste, jak udzielenie zgody. W przeciwnym razie mechanizm zgody administratora nie spełnia wymogów RODO[29].
- równoważenie interesów – w przypadku gdy podstawą prawną są prawnie uzasadnione interesy, administrator musi przeprowadzić wyważone równoważenie interesów, zwracając szczególną uwagę na brak równowagi sił, zwłaszcza w przypadku dzieci poniżej 18. roku życia i innych grup szczególnie wrażliwych. Muszą istnieć środki i zabezpieczenia mające na celu złagodzenie negatywnego wpływu na osoby, których dane dotyczą.
- ustalenie z góry – podstawa prawna jest ustalana przed rozpoczęciem przetwarzania danych;
- ustanie – jeżeli podstawa prawna przestaje mieć zastosowanie, należy odpowiednio przerwać przetwarzanie;
- dostosowanie – jeżeli nastąpiła ważna zmiana podstawy prawnej przetwarzania, faktyczne przetwarzanie należy dostosować zgodnie z nową podstawą prawną[30].
- podział odpowiedzialności – ilekroć przewiduje się współadministrowanie, strony muszą w wyraźny i przejrzysty sposób rozdzielić swoje właściwe obowiązki w stosunku do osoby, której dane dotyczą, oraz zaprojektować środki przetwarzania danych zgodnie z tym podziałem.

Przykład

Bank planuje zaoferować usługę w celu zwiększenia skuteczności zarządzania wnioskami kredytowymi. Założeniem usługi jest to, że bank, zwracając się do klienta o zgodę, jest w stanie pobrać dane o kliencie bezpośrednio od publicznych organów podatkowych. Niniejszy przykład nie uwzględnia przetwarzania danych osobowych z innych źródeł.

Pozyskanie danych osobowych dotyczących sytuacji finansowej osoby, której dane dotyczą, jest niezbędne do podjęcia działań na jej wniosek przed zawarciem umowy kredytowej[31]. Zbieranie danych osobowych bezpośrednio od organów podatkowych nie jest jednak uważane za konieczne, ponieważ klient może zawrzeć umowę, udostępniając informacje od organów podatkowych we własnym zakresie. Mimo że bank może mieć uzasadniony interes w uzyskaniu dokumentacji bezpośrednio od organów podatkowych, na przykład w celu zapewnienia skuteczności przetwarzania kredytu, udzielenie bankom takiego bezpośredniego dostępu do danych osobowych wnioskodawców stanowi ryzyko związane z wykorzystaniem lub potencjalnym nadużyciem praw dostępu.

[27] Zobacz sekcja dotycząca ograniczenia celu poniżej.
[28] Zob. wytyczne 05/2020 dotyczące zgody na mocy rozporządzenia 2016/679. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_pl
[29] Zob. wytyczne 05/2020 dotyczące na mocy rozporządzenia 2016/679, s. 24. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_pl
[30] W przypadku gdy pierwotną podstawą prawną jest zgoda, zob. wytyczne 05/2020 dotyczące zgody na mocy rozporządzenia 2016/679. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_pl
[31] Zobacz art. 6 ust. 1 lit. b) RODO.

Realizując zasadę zgodności z prawem, administrator ma świadomość, że nie może wykorzystywać sformułowania „niezbędne do zawarcia umowy" w odniesieniu do tej części przetwarzania, która polega na gromadzeniu danych osobowych bezpośrednio od organów podatkowych. Fakt, że ten konkretny proces przetwarzania niesie ze sobą ryzyko mniejszego zaangażowania osoby, której dane dotyczą, w przetwarzanie jej danych, jest również istotnym czynnikiem w ocenie zgodności z prawem samego przetwarzania. Bank uznaje, że ta część przetwarzania musi opierać się na innej podstawie prawnej przetwarzania. W danym państwie członkowskim, w którym znajduje się siedziba administratora danych, istnieją przepisy krajowe umożliwiające bankowi bezpośrednie gromadzenie informacji od publicznych organów podatkowych, jeżeli osoba, której dane dotyczą, wyrazi na to wcześniej zgodę.

Bank przedstawia zatem informacje dotyczące przetwarzania danych na internetowej platformie do składania wniosków w sposób ułatwiający osobom, których dane dotyczą, zrozumienie, jaki zakres przetwarzania jest obowiązkowy, a jaki opcjonalny. Opcje przetwarzania domyślnie nie pozwalają na pozyskiwanie danych bezpośrednio ze źródeł innych niż sama osoba, której dane dotyczą, a możliwość bezpośredniego pozyskiwania informacji jest przedstawiona w sposób, który nie zniechęca osoby, której dane dotyczą, do wstrzymania się od tej czynności. Każda zgoda na zbieranie danych bezpośrednio od innych administratorów jest tymczasowym prawem dostępu do określonego zbioru informacji.

Każda udzielona zgoda jest przetwarzana elektronicznie w sposób umożliwiający dokumentację, a osobom, których dane dotyczą, przestawia się łatwy sposób kontrolowania tego, na co wyraziły zgodę, oraz wycofania tej zgody.

Administrator wcześniej ocenił te wymogi w zakresie ochrony danych w fazie projektowania oraz domyślnej ochrony danych i uwzględnił wszystkie te kryteria w swojej specyfikacji wymagań do celów przetargu na zakup platformy. Administrator jest świadomy faktu, że jeżeli nie uwzględni wymogów w zakresie ochrony danych w fazie projektowania oraz domyślnej ochrony danych w przetargu, później może być już zbyt późno na wdrożenie ochrony danych lub proces ten może być bardzo kosztowny.

3.3 Rzetelność

69. Rzetelność jest nadrzędną zasadą, która wymaga, aby dane osobowe nie były przetwarzane w sposób, który jest bezzasadnie szkodliwy, dyskryminujący, nieoczekiwany lub wprowadzający w błąd względem osoby, której dane dotyczą. Środki i zabezpieczenia, dzięki którym realizowana jest zasada rzetelności, wspierają również prawa i wolności osób, których dane dotyczą, szczególnie prawo do informacji (przejrzystości), prawo do interwencji (dostępu, usuwania, przenoszenia, sprostowania danych) oraz prawo do ograniczenia przetwarzania (prawo do niepodlegania zautomatyzowanemu podejmowaniu decyzji w indywidualnych przypadkach oraz niedyskryminacja osób, których dane dotyczą, w takich procesach).

70. Kluczowe elementy uwzględniania ochrony danych w fazie projektowania i domyślnej ochrony danych w stosunku do rzetelności mogą obejmować:
    - autonomię – osobom, których dane dotyczą, należy przyznać najwyższy zakres autonomii, aby mogły decydować o sposobie wykorzystania ich danych osobowych, a także o zakresie i warunkach tego wykorzystania lub przetwarzania;
    - interakcję – osoby, których dane dotyczą, muszą mieć możliwość informowania o swoich prawach i korzystania z nich w odniesieniu do danych osobowych przetwarzanych przez administratora danych;

- oczekiwania – przetwarzanie powinno odpowiadać uzasadnionym oczekiwaniom osób, których dane dotyczą;
- niedyskryminację – administrator nie może niesprawiedliwie dyskryminować osoby, której dane dotyczą;
- niewykorzystywanie – administrator nie może wykorzystywać potrzeb ani słabości osób, których dane dotyczą;
- wybór konsumenta – administrator nie powinien uzależniać swoich użytkowników od jednego dostawcy w nieuczciwy sposób. W przypadku gdy usługa przetwarzania danych osobowych jest zastrzeżona, może to doprowadzić do „zablokowania" użytkownika w korzystaniu z usługi, które nie jest uczciwe, jeśli utrudnia osobom, których dane dotyczą, korzystanie z prawa do przenoszenia danych zgodnie z art. 20;
- równowagę sił – równowaga sił powinna być kluczowym celem relacji między administratorem a osobą, której dane dotyczą. Należy unikać nierównowagi sił. Jeśli nie jest to jednak możliwe, należy ją stwierdzić i wyjaśnić za pomocą odpowiednich środków zaradczych;
- brak przeniesienia ryzyka – administratorzy nie powinni przenosić ryzyka związanego z przedsiębiorstwem na osoby, których dane dotyczą;
- brak oszustw – informacje na temat przetwarzania danych i ich opcje należy przekazywać w sposób obiektywny i neutralny, unikając wszelkich mylących lub manipulujących sformułowań lub konstrukcji;
- poszanowanie praw – administrator musi przestrzegać podstawowych praw osób, których dane dotyczą oraz wdrażać odpowiednie środki i zabezpieczenia, a także nie może naruszać tych praw, chyba że jest to wyraźnie uzasadnione przez prawo;
- etykę – administrator powinien dostrzegać szerszy wpływ przetwarzania na prawa i godność osób fizycznych;
- prawdę – administrator jest zobowiązany do udostępnienia informacji na temat sposobu, w jaki przetwarza dane osobowe, oraz powinien działać tak, jak zadeklarował i nie wprowadzać w błąd osób, których dane dotyczą;
- interwencję człowieka – administrator musi uwzględnić *wykwalifikowaną* interwencję człowieka, dzięki której możliwe będzie wykrywanie błędów stronniczości, jakie maszyny mogą popełniać, zgodnie z prawem do niepodlegania zautomatyzowanemu podejmowaniu decyzji w indywidualnych przypadkach określonym w art. 22[32];
- uczciwe algorytmy – systematyczna ocena funkcjonowania algorytmów zgodnie z celami i dostosowanie algorytmów, aby ograniczyć wykryte uprzedzenia i zapewnić rzetelność w procesie przetwarzania. Osobom, których dane dotyczą, powinno się przekazywać informacje na temat funkcjonowania przetwarzania danych osobowych w oparciu o algorytmy analizujące lub prognozujące aspekty dotyczące tych osób, takie jak ich efekty pracy, sytuacja ekonomiczna, zdrowie, osobiste preferencje, wiarygodność lub zachowanie, lokalizacja lub przemieszczanie się[33].

Przykład 1

[32] Zob. wytyczne w sprawie zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania do celów rozporządzenia 2016/679.
https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49826
[33] Zobacz motyw 71 RODO.

Administrator obsługuje wyszukiwarkę internetową, która przetwarza głównie dane osobowe tworzone przez użytkowników. Administrator czerpie korzyści z posiadania dużej ilości danych osobowych oraz z możliwości wykorzystania ich do celów stosowania ukierunkowanych reklam. Administrator chce zatem wpłynąć na osoby, których dane dotyczą, aby zezwoliły na zbieranie i wykorzystywanie ich danych osobowych na szeroką skalę. Zgodę należy uzyskać poprzez przedstawienie opcji przetwarzania osobie, której dane dotyczą.

Realizując zasadę rzetelności, z uwzględnieniem charakteru, zakresu, kontekstu i celu przetwarzania, administrator ma świadomość, że nie może przedstawiać opcji w sposób nakłaniający osobę, której dane dotyczą, do zezwolenia administratorowi na zbieranie większej ilości danych osobowych niż w przypadku, gdyby opcje te przedstawiono w sposób jednakowy i neutralny. Oznacza to, że administratorzy nie mogą przedstawiać opcji przetwarzania w sposób utrudniający osobom, których dane dotyczą, wstrzymanie się od udostępniania swoich danych lub dostosowanie ich ustawień prywatności i ograniczenie przetwarzania. Są to przykłady złych wzorców, które są sprzeczne z duchem art. 25. Domyślne opcje przetwarzania nie powinny być inwazyjne, a możliwość wyboru dalszego przetwarzania powinna być przedstawiona w sposób, który nie wywiera presji na osobie, której dane dotyczą, aby wyraziła zgodę. Z tego względu administrator przedstawia opcje wyrażenia zgody lub wstrzymania się od jej udzielenia jako dwie równie widoczne możliwości wyboru, odpowiednio przedstawiające następstwa wyboru każdej z nich dla osoby, której dane dotyczą.

Przykład 2

Inny administrator przetwarza dane osobowe w celu świadczenia usługi przesyłania strumieniowego, w ramach której użytkownicy mogą wybrać między zwykłą subskrypcją o standardowej jakości a subskrypcją premium o wyższej jakości. W ramach subskrypcji premium subskrybenci otrzymują priorytetową obsługę klienta.

W odniesieniu do zasady rzetelności, priorytetowa obsługa klienta przyznana abonentom premium nie może dyskryminować stałych abonentów w zakresie dostępu do korzystania z ich praw zgodnie z art. 12 RODO. Oznacza to, że chociaż subskrybenci opcji premium otrzymują priorytetową obsługę, takie priorytetowe traktowanie nie może skutkować brakiem odpowiednich środków umożliwiających udzielenie odpowiedzi na wnioski od zwykłych subskrybentów bez zbędnej zwłoki, a w każdym razie w ciągu jednego miesiąca od otrzymania wniosków.

Klienci traktowani priorytetowo mogą płacić za lepszą obsługę, ale wszystkie osoby, których dane dotyczą, mają równy i niezróżnicowany dostęp do korzystania ze swoich praw i wolności zgodnie z wymogami art. 12.

3.4 Ograniczenie celu[34]

71. Administrator jest zobowiązany do zbierania danych w konkretnych, wyraźnych i prawnie uzasadnionych celach oraz do nieprzetwarzania ich dalej w sposób niezgodny z celami, w jakich zostały

[34] Grupa Robocza Art. 29 przedstawiła wytyczne dotyczące zrozumienia zasady ograniczenia celu na mocy dyrektywy 95/46/WE. Chociaż EROD nie przyjęła przedmiotowej opinii, może ona być nadal istotna, ponieważ brzmienie zasady w ramach RODO jest takie samo. Grupa Robocza Art. 29. „Opinia 03/2013 w sprawie ograniczenia celu". WP 203, 2 kwietnia 2013 r. ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

zebrane[35]. Projektowanie przetwarzania powinno być zatem kształtowane przez to, co niezbędne do osiągnięcia tych celów. Jeżeli dalsze przetwarzanie danych ma mieć miejsce, administrator musi najpierw upewnić się, że cele tego przetwarzania są zgodne z celami pierwotnymi, oraz odpowiednio zaprojektować takie przetwarzanie. Niezależnie od tego, czy nowy cel jest zgodny z celem pierwotnym, należy poddać go ocenie według kryteriów określonych w art. 6 ust. 4.

72. Kluczowe elementy uwzględniania ochrony danych w fazie projektowania i domyślnej ochrony danych w stosunku do ograniczenia celu mogą obejmować:
- ustalenie z góry – prawnie uzasadnione cele należy określić przed zaprojektowaniem przetwarzania;
- specyfikę – podane są konkretne i wyraźne cele, w których przetwarzane są dane osobowe.
- ukierunkowanie na cel – cel przetwarzania powinien kierować projektowaniem przetwarzania i stanowić podstawę granic przetwarzania;
- niezbędność – na podstawie celu określa się, jakie dane osobowe są niezbędne do przetwarzania;
- zgodność – każdy nowy cel musi być zgodny z celem pierwotnym, dla którego zebrano dane, i musi prowadzić do istotnych zmian w projekcie;
- ograniczenie dalszego przetwarzania – administrator nie powinien łączyć zbiorów danych ani dokonywać dalszego przetwarzania w nowych, niezgodnych celach;
- ograniczenie ponownego wykorzystania – administrator powinien stosować środki techniczne, w tym haszowanie (ang. hashing) i szyfrowanie, w celu ograniczenia możliwości ponownego wykorzystania danych osobowych w innym celu. Administrator powinien również dysponować środkami organizacyjnymi, takimi jak strategie i zobowiązania umowne, które ograniczają możliwość ponownego, nieuprawnionego wykorzystania danych osobowych;
- przegląd – administrator ma obowiązek regularnie sprawdzać, czy przetwarzanie jest niezbędne do celów, dla których zebrano dane, a także testować projekt pod względem ograniczenia celu;

Przykład

Administrator przetwarza dane osobowe swoich klientów. Celem przetwarzania danych jest realizacja zamówienia, tj. dostarczenie towarów pod właściwy adres i otrzymanie zapłaty. Przechowywane dane osobowe obejmują historię zamówień, imię i nazwisko, adres, adres e-mail i numer telefonu.

Administrator rozważa zakup produktu przeznaczonego do zarządzania relacjami z klientami (CRM), który gromadzi wszystkie dane dotyczące klienta, takie jak sprzedaż, marketing i obsługa klienta, w jednym miejscu. Produkt umożliwia przechowywanie informacji na temat wszystkich połączeń telefonicznych, działań, dokumentów, wiadomości e-mail i kampanii marketingowych w celu uzyskania pełnego obrazu klienta. Dodatkowo, CRM może automatycznie analizować siłę nabywczą klientów poprzez wykorzystanie informacji publicznych. Celem analizy jest lepsze ukierunkowanie działań reklamowych. Działania te nie wchodzą w zakres pierwotnego, zgodnego z prawem celu przetwarzania danych.

Aby zachować zgodność z zasadą ograniczenia celu, administrator danych wymaga od dostawcy produktu, aby przedstawił mapę różnych działań związanych z przetwarzaniem, które wykorzystują dane osobowe do celów istotnych dla administratora.

[35] Artykuł 5 ust. 1 lit. b) RODO.

Po otrzymaniu wyników takiego mapowania administrator ocenia, czy nowy cel marketingowy i cel reklamy ukierunkowanej są zgodne z pierwotnymi celami określonymi w momencie zbierania danych oraz czy istnieje wystarczająca podstawa prawna do ich przetwarzania. Jeżeli ocena ta nie daje pozytywnej odpowiedzi, administrator nie wykorzystuje dalej odnośnych właściwości. Ewentualnie administrator może zrezygnować z oceny i nie korzystać z opisanych właściwości produktu.

3.5 Minimalizacja danych

73. Jedynie dane osobowe, które są adekwatne, stosowne oraz ograniczone do tego, co niezbędne do osiągnięcia celu, są przetwarzane[36]. W rezultacie administrator musi z góry określić, które cechy i parametry systemów przetwarzania oraz ich funkcje pomocnicze są dopuszczalne. Minimalizacja danych uzasadnia i urzeczywistnia zasadę konieczności (niezbędności). W ramach dalszego przetwarzania administrator powinien okresowo rozważać, czy przetwarzane dane osobowe nadal są adekwatne, stosowne i ograniczone do tego, co niezbędne, oraz czy dane należy usunąć lub zanonimizować.

74. Przede wszystkim administratorzy muszą ustalić, czy w ogóle muszą przetwarzać dane osobowe do swoich odpowiednich celów. Administrator powinien sprawdzić, czy odpowiednie cele można osiągnąć, przetwarzając mniej danych osobowych lub posiadając mniej szczegółowe lub zagregowane dane osobowe, lub w ogóle bez konieczności przetwarzania danych osobowych[37]. Weryfikacja taka powinna mieć miejsce przed jakimkolwiek przetwarzaniem, ale może być również przeprowadzona w dowolnym momencie tego procesu. Jest to również zgodne z art. 11.

75. Minimalizacja może również odnosić się do stopnia identyfikacji. Jeżeli cel przetwarzania nie wymaga, aby ostateczny zbiór danych odnosił się do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej (jak w przypadku statystyk), ale wymaga tego pierwotne przetwarzanie (np. przed agregacją danych), administrator usuwa lub anonimizuje dane osobowe, gdy tylko identyfikacja nie jest już konieczna. Ewentualnie, jeżeli dalsza identyfikacja jest konieczna w odniesieniu do innych czynności przetwarzania, dane osobowe należy spseudonimizować, aby zminimalizować ryzyko naruszenia praw osób, których dane dotyczą.

76. Kluczowe elementy uwzględniania ochrony danych w fazie projektowania i domyślnej ochrony danych w stosunku do minimalizacji danych mogą obejmować:
- unikanie przetwarzania danych – całkowite unikanie przetwarzania danych osobowych, jeżeli jest to możliwe w określonym celu;
- ograniczenie – ograniczenie ilości zbieranych danych osobowych do ilości niezbędnej do osiągnięcia danego celu;
- ograniczenie dostępu – kształtowanie przetwarzania danych w taki sposób, aby minimalna liczba osób wymagała dostępu do danych osobowych w celu wykonywania swoich obowiązków, a także odpowiednie ograniczenie dostępu;
- stosowność – dane osobowe mają znaczenie dla danego przetwarzania, a administrator musi być w stanie tę stosowność wykazać;

[36] Artykuł 5 ust. 1 lit. c) RODO.
[37] Motyw 39 RODO stanowi: „Dane osobowe powinny być przetwarzane tylko w przypadkach, gdy celu przetwarzania nie można w rozsądny sposób osiągnąć innymi sposobami".

- niezbędność – każda kategoria danych osobowych jest niezbędna do osiągnięcia określonych celów i powinna być przetwarzana tylko wtedy, gdy osiągnięcie tego celu w inny sposób nie jest możliwe;
- agregację – używanie zagregowanych danych, o ile to możliwe;
- pseudonimizację – gdy tylko posiadanie danych osobowych umożliwiających bezpośrednią identyfikację nie jest już konieczne, dane należy spseudonimizować, a klucze do identyfikacji przechowywać oddzielnie;
- anonimizację i usuwanie – w przypadku gdy dane osobowe nie są lub przestały być niezbędne do osiągnięcia celu, dane osobowe są anonimizowane lub usuwane;
- przepływ danych – przepływ danych musi być na tyle skuteczny, aby nie tworzyć większej liczby kopii niż jest to konieczne;
- „stan wiedzy technicznej"– administrator danych powinien stosować aktualne i odpowiednie technologie, aby ograniczyć i zminimalizować ilość danych.

Przykład 1

Księgarnia chce zwiększyć swoje dochody, sprzedając książki przez Internet. Właściciel księgarni chce opracować standardowy formularz dotyczący procesu zamawiania. Aby zapewnić sobie, że klient udzieli wszystkich potrzebnych informacji, właściciel księgarni wprowadza w formularzu wymóg wypełnienia wszystkich pól (jeśli klient nie wypełni wszystkich pól, nie będzie mógł złożyć zamówienia). Właściciel księgarni początkowo korzysta ze standardowego formularza kontaktowego, w którym klient proszony jest o podanie daty urodzenia, numeru telefonu i adresu zamieszkania. Nie wszystkie pola w formularzu są jednak bezwzględnie niezbędne do osiągnięcia celu, jakim jest zakup i dostawa książek. W tym konkretnym przypadku, jeżeli osoba, której dane dotyczą, płaci za produkt z góry, jej data urodzenia i numer telefonu nie są konieczne do zrealizowania zakupu produktu. Oznacza to, że pola te nie mogą być obowiązkowo wypełniane w formularzu internetowym na potrzeby zamówienia produktu, chyba że administrator danych potrafi wyraźnie uzasadnić, dlaczego dane te są niezbędne. Ponadto istnieją sytuacje, w których adres nie będzie niezbędny. Na przykład, zamawiając e-book, klient może pobrać produkt bezpośrednio na swoje urządzenie.

Właściciel sklepu internetowego podejmuje zatem decyzję o stworzeniu dwóch formularzy internetowych: formularza służącego do zamawiania książek, z polem dotyczącym adresu klienta, i formularza służącego do zamawiania książek elektronicznych, bez pola dotyczącego adresu klienta.

Przykład 2

Przedsiębiorstwo transportu publicznego pragnie zebrać informacje statystyczne w oparciu o trasy podróżnych. Jest to przydatne do celów dokonywania właściwych wyborów dotyczących zmian harmonogramów transportu publicznego i właściwych tras pociągów. Pasażerowie muszą przeciągnąć bilet przez czytnik za każdym razem, gdy wchodzą do środka transportu lub go opuszczają. Po przeprowadzeniu oceny ryzyka związanego z prawami i swobodami pasażerów w zakresie gromadzenia danych o trasach podróży, administrator danych stwierdza, że może ustalić tożsamość pasażerów w sytuacji, gdy mieszkają lub pracują na obszarach słabo zaludnionych, na podstawie pojedynczej trasy, za pomocą kodu identyfikacyjnego biletu. W związku z tym, ponieważ nie jest to niezbędne dla osiągnięcia celu optymalizacji harmonogramów transportu publicznego i tras pociągów, administrator

nie przechowuje identyfikatora biletu. Po zakończeniu podróży administrator przechowuje jedynie informacje dotyczące poszczególnych tras podróży, aby nie móc zidentyfikować podróży powiązanych z danym biletem, a jedynie zatrzymać informacje dotyczące odrębnych tras podróży.

W przypadkach, kiedy nadal może istnieć ryzyko ustalenia tożsamości osoby jedynie na podstawie trasy jej przejazdu transportem publicznym, administrator wprowadza środki statystyczne w celu zmniejszenia ryzyka, takie jak skrócenie początku i końca trasy.

Przykład 3

Celem kuriera jest przeprowadzenie oceny skuteczności dostaw pod kątem czasu dostawy, harmonogramu nakładu pracy i zużycia paliwa. Aby osiągnąć ten cel, kurier musi przetworzyć szereg danych osobowych dotyczących zarówno pracowników (kierowców), jak i klientów (adresy, przedmioty do dostarczenia itp.). Ta operacja przetwarzania pociąga za sobą ryzyko związane zarówno z monitorowaniem pracowników, które wymaga szczególnych zabezpieczeń prawnych, jak i ze śledzeniem nawyków klientów przy użyciu informacji na temat dostarczonych przedmiotów. Ryzyko to można znacznie ograniczyć za pomocą odpowiedniej pseudonimizacji pracowników i klientów. W szczególności, jeżeli klucze pseudonimizacji są często zmieniane, a zamiast szczegółowych adresów uwzględniane są obszary makro, dąży się do skutecznej minimalizacji danych, a administrator może skoncentrować się wyłącznie na procesie dostawy oraz na osiągnięciu celu optymalizacji zasobów, bez przekraczania progu monitorowania zachowań poszczególnych osób (klientów lub pracowników).

Przykład 4

Szpital gromadzi dane o swoich pacjentach w systemie informacji szpitalnej (elektroniczna karta zdrowia). Personel szpitala korzysta z dokumentacji medycznej pacjentów w celu podejmowania decyzji dotyczących opieki nad nimi i ich leczenia, a także aby udokumentować wszystkie podejmowane działania diagnostyczne, opiekuńcze i lecznicze. Domyślnie dostęp uzyskują jedynie ci członkowie personelu medycznego, którzy są przypisani do danego pacjenta na oddziale specjalistycznym, na którym przebywa pacjent. Grupa osób mających dostęp do dokumentacji pacjenta powiększa się, jeżeli w procesie leczenia uczestniczą inne oddziały lub jednostki diagnostyczne. Po wypisaniu pacjenta ze szpitala i dokonaniu rozliczeń, dostęp do jego dokumentacji zostaje ograniczony do niewielkiej grupy pracowników danego oddziału specjalistycznego, którzy – za zgodą pacjenta – udzielają informacji medycznych lub konsultacji, o które proszą inni dostawcy usług medycznych.

3.6 Prawidłowość

77. Dane osobowe muszą być prawidłowe i uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane[38].

78. Wymogi należy oceniać w kontekście ryzyka i konsekwencji faktycznego wykorzystania danych. Nieprawidłowe dane osobowe mogą powodować ryzyko naruszenia praw i wolności osób, których

[38] Artykuł 5 ust. 1 lit. d) RODO.

dane dotyczą, na przykład gdy prowadzą do błędnej diagnozy lub niewłaściwego traktowania protokołu zdrowia, lub błędny obraz osoby może prowadzić do podejmowania decyzji na niewłaściwej podstawie przy przetwarzaniu ręcznym, przy użyciu zautomatyzowanego procesu decyzyjnego albo sztucznej inteligencji.

79. Kluczowe elementy uwzględniania ochrony danych w fazie projektowania i domyślnej ochrony danych w stosunku do prawidłowości mogą obejmować:
- źródło danych – źródła danych osobowych powinny być wiarygodne pod względem prawidłowości danych;
- stopień prawidłowości – każdy element danych osobowych musi być na tyle prawidłowy, na ile jest to niezbędne do osiągnięcia określonych celów;
- mierzalną prawidłowość – zmniejszenie liczby fałszywych wyników dodatnich/ujemnych, na przykład stronniczości w zautomatyzowanych decyzjach i sztucznej inteligencji;
- weryfikację – w zależności od charakteru danych, w odniesieniu do tego, jak często może się on zmieniać, administrator powinien weryfikować poprawność danych osobowych z osobą, której dane dotyczą, przed rozpoczęciem przetwarzania i na różnych jego etapach (np. w zależności od kryterium wieku);
- usuwanie/sprostowanie – administrator musi usunąć lub sprostować nieprawidłowe dane bez zbędnej zwłoki. Administrator musi w szczególności ułatwić tę operację, jeśli osoby, których dane dotyczą, są lub były dziećmi i w późniejszym okresie chcą usunąć takie dane osobowe[39].
- unikanie powielania błędów – administratorzy powinni ograniczać skutki skumulowanych błędów w łańcuchu przetwarzania;
- dostęp – osoby, których dane dotyczą, powinny otrzymywać informacje na temat danych osobowych i skuteczny dostęp do nich zgodnie z art. 12–15 RODO, aby mogły kontrolować ich poprawność i w razie potrzeby je sprostować;
- ciągłą prawidłowość – dane osobowe powinny być prawidłowe na wszystkich etapach przetwarzania; testy dotyczące prawidłowości należy przeprowadzać na krytycznych etapach;
- aktualizację – dane osobowe muszą być aktualizowane, jeżeli jest to niezbędne do osiągnięcia celu;
- projektowanie danych – zastosowanie właściwości technologicznych i organizacyjnych projektu w celu zmniejszenia nieprawidłowości, na przykład przedstawienie zwięzłych, z góry określonych opcji wyboru zamiast wolnych pól tekstowych.

Przykład 1

Firma ubezpieczeniowa chciałaby wykorzystać sztuczną inteligencję (SI) do profilowania klientów wykupujących ubezpieczenie jako podstawę do podejmowania decyzji przy obliczaniu ryzyka ubezpieczeniowego. Określając sposób, w jaki należy opracować rozwiązania z zakresu SI, firma określa sposoby przetwarzania i powinna uwzględnić ochronę danych w fazie projektowania przy wyborze SI od sprzedawcy oraz przy podejmowaniu decyzji o sposobie szkolenia SI.

W przypadku określania sposobu szkolenia SI administrator musi dysponować prawidłowymi danymi, aby osiągnąć dokładne wyniki. W związku z tym administrator musi zapewnić, aby dane stosowane do celów szkolenia SI były prawidłowe.

Zakładając, że istnieje ważna podstawa prawna do szkolenia SI z wykorzystaniem danych osobowych pochodzących z dużego pod-zbioru obecnych klientów, administrator wybiera pulę klientów będących przedstawicielami danej populacji, aby uniknąć błędu.

[39] Por. motyw 65.

Dane klientów są następnie pobierane z odpowiedniego systemu obsługi danych, w tym dane dotyczące rodzaju ubezpieczenia, np. ubezpieczenie zdrowotne, ubezpieczenie domu, ubezpieczenie podróżne itp. oraz dane z rejestrów publicznych, do których mają zgodnie z prawem dostęp. Wszystkie dane są pseudonimizowane przed przekazaniem ich do systemu stworzonego na potrzeby szkolenia modelu SI.

W celu zapewnienia, aby dane wykorzystane do szkolenia SI były możliwie najbardziej prawidłowe, administrator zbiera jedynie dane pochodzące ze źródeł danych z poprawnymi i aktualnymi informacjami.

Firma ubezpieczeniowa sprawdza, czy SI jest wiarygodna i zapewnia niedyskryminujące wyniki zarówno podczas opracowywania produktu, jak i ostatecznie przed jego wprowadzeniem na rynek. W przypadku gdy SI jest w pełni przeszkolona i sprawnie działająca, zakład ubezpieczeń wykorzystuje wyniki, aby uzupełnić ocenę ryzyka ubezpieczeniowego, nie opierając się jednak wyłącznie na SI przy podejmowaniu decyzji o przyznaniu ubezpieczenia, chyba że decyzja została podjęta zgodnie z wyjątkami określonymi w art. 22 ust. 2 RODO.

Zakład ubezpieczeń będzie również systematycznie dokonywać przeglądu wyników SI, aby zachować wiarygodność i w razie konieczności dostosować algorytm.

Przykład 2

Administratorem danych jest instytucja zdrowia publicznego poszukująca metod służących zapewnieniu integralności i prawidłowości danych osobowych w rejestrach klientów.

W sytuacjach gdy dwie osoby przybywają do instytucji w tym samym czasie i otrzymują jednakowe leczenie, istnieje ryzyko pomylenia tych dwóch osób, jeżeli jedynym parametrem, który je różni, jest ich imię i nazwisko. W celu zapewnienia prawidłowości administrator potrzebuje niepowtarzalnego identyfikatora dla każdej osoby, a zatem większej ilości informacji niż tylko imienia i nazwiska klienta.

Instytucja korzysta z szeregu systemów zawierających dane osobowe klientów i musi zapewnić, aby dane związane z klientem były zawsze poprawne, prawidłowe i zgodne we wszystkich systemach. Instytucja wyodrębniła kilka zagrożeń, jakie mogą wystąpić w przypadku zmiany informacji w jednym systemie, przy jednoczesnym braku zmian w innych systemach.

Administrator podejmuje decyzję o zminimalizowaniu ryzyka przez wykorzystanie techniki haszowania zapewniającej integralność danych w dzienniku leczenia. Dla zapisów w dziennikach leczenia i związanych z nimi klientów tworzone są stałe kryptograficzne znaczniki czasu, tak aby w razie potrzeby można było rozpoznać, skorelować i prześledzić wszelkie zmiany.

3.7 Ograniczenie przechowywania

80. Administrator musi zapewnić, aby dane osobowe były przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane[40].

[40] Artykuł 5 ust. 1 lit. c) RODO.

Istotne jest, aby administrator dokładnie wiedział, jakie dane osobowe są przetwarzane przez przedsiębiorstwo i w jakim celu. Cel przetwarzania jest głównym kryterium decydującym o tym, jak długo dane osobowe są przechowywane.

81. Środki i zabezpieczenia przyczyniające się do realizacji zasady ograniczenia przechowywania uzupełniają prawa i wolności osób, których dane dotyczą, w szczególności prawo do usunięcia danych i prawo sprzeciwu.

82. Kluczowe elementy uwzględniania ochrony danych w fazie projektowania i domyślnej ochrony danych w stosunku do ograniczenia przechowywania mogą obejmować:
    - usuwanie i anonimizację – administrator powinien posiadać jasne wewnętrzne procedury i możliwości usuwania lub anonimizacji;
    - skuteczność anonimizacji/usuwania – administrator musi zapewnić, aby ponowna identyfikacja zanonimizowanych danych lub odzyskanie usuniętych danych nie były możliwe, a także powinien weryfikować, czy jest to możliwe;
    - automatyzację – usuwanie określonych danych osobowych powinno odbywać się w zautomatyzowany sposób;
    - kryteria przechowywania – administrator ma obowiązek określić, jakie dane są niezbędne do osiągnięcia danego celu i jak długo należy je przechowywać;
    - uzasadnienie – administrator danych powinien umieć uzasadnić, dlaczego okres przechowywania jest niezbędny dla danego celu i danych osobowych oraz wykazać podstawy prawne takiego okresu przechowywania;
    - egzekwowanie zasad polityki w zakresie zatrzymywania danych – administrator ma obowiązek egzekwować realizację zasad wewnętrznej polityki zatrzymywania danych oraz weryfikować, czy organizacja stosuje zasady tej polityki;
    - kopie zapasowe/rejestry – administratorzy ustalają dane osobowe niezbędne do tworzenia kopii zapasowych i rejestrów oraz czas ich przechowywania;
    - przepływ danych – administratorzy powinni zwracać uwagę na przepływ danych osobowych i przechowywanie wszelkich ich kopii oraz dążyć do ograniczenia ich „tymczasowego" przechowywania.

Przykład

Administrator danych gromadzi dane osobowe, jeżeli celem przetwarzania jest zarządzanie członkostwem osoby, której dane dotyczą. Dane osobowe są usuwane po zakończeniu członkostwa i nie ma podstawy prawnej do ich dalszego przechowywania.

Administrator opracowuje wewnętrzną procedurę dotyczącą zatrzymywania i usuwania danych. Zgodnie z powyższym pracownicy muszą ręcznie usuwać dane osobowe po upływie okresu zatrzymywania danych. Pracownicy przestrzegają procedury, zgodnie z którą regularnie korygują i usuwają dane ze wszelkich urządzeń, kopii zapasowych, rejestrów, wiadomości e-mail i innych odpowiednich nośników danych.

Aby zapewnić skuteczniejsze usuwanie danych i zmniejszyć podatność na błędy, administrator wdraża automatyczny system w celu zautomatyzowanego, rzetelnego i bardziej systematycznego usuwania danych. System jest skonfigurowany tak, aby działał zgodnie z określoną procedurą usuwania danych, która jest powtarzana w określonych z góry, regularnych odstępach czasu i służy usuwaniu danych osobowych ze wszystkich nośników danych przedsiębiorstwa. Administrator regularnie dokonuje przeglądu i testowania procedury zatrzymywania danych oraz zapewnia jej zgodność z aktualną polityką zatrzymywania danych.

3.8 Integralność i poufność

83. Zasada integralności i poufności obejmuje ochronę danych przed nieuprawnionym lub niezgodnym z prawem przetwarzaniem oraz przed przypadkową utratą, zniszczeniem lub uszkodzeniem, przy zastosowaniu odpowiednich środków technicznych lub organizacyjnych. Bezpieczeństwo danych osobowych wymaga odpowiednich środków, których celem jest zapobieganie przypadkom naruszenia ochrony danych i zarządzanie nimi; zagwarantowanie właściwej realizacji zadań związanych z przetwarzaniem danych oraz zgodności z innymi zasadami; a także ułatwienie skutecznego korzystania z praw przysługujących osobom fizycznym.

84. W motywie 78 stwierdzono, że jeden ze środków w zakresie ochrony danych w fazie projektowania oraz domyślnej ochrony danych może polegać na umożliwieniu administratorowi „tworzenia i doskonalenia zabezpieczeń". W motywie 78, oprócz stosowania innych środków w zakresie ochrony danych w fazie projektowania oraz domyślnej ochrony danych, sugeruje się, aby administratorzy byli odpowiedzialni za ciągłą ocenę tego, czy za każdym razem stosowane są odpowiednie sposoby przetwarzania oraz czy wybrane środki faktycznie przeciwdziałają istniejącym słabym punktom. Ponadto administratorzy danych powinni przeprowadzać regularne przeglądy środków bezpieczeństwa informacji zapewniających ochronę danym osobowym, a także procedur postępowania w przypadku naruszenia ochrony danych.

85. Kluczowe elementy uwzględniania ochrony danych w fazie projektowania i domyślnej ochrony danych w stosunku do integralności i poufności mogą obejmować:
    - system zarządzania bezpieczeństwem informacji (SZBI) – posiadanie środków operacyjnych w ramach polityki zarządzania oraz procedur w zakresie bezpieczeństwa informacji;
    - analizę ryzyka – ocena zagrożeń dla bezpieczeństwa danych osobowych polegająca na analizie wpływu na prawa osób fizycznych i przeciwdziałaniu zidentyfikowanym zagrożeniom. Możliwość wykorzystania w ocenie ryzyka; opracowanie i utrzymanie kompleksowego, systematycznego i realistycznego „modelowania zagrożeń" oraz analizy obszaru ataku zaprojektowanego oprogramowania w celu ograniczenia wektorów ataku i możliwości wykorzystania słabych punktów;
    - bezpieczeństwo w fazie projektowania – uwzględnienie wymogów bezpieczeństwa na jak najwcześniejszym etapie projektowania i rozwoju systemu oraz ciągła integracja i wykonywanie odpowiednich testów;
    - utrzymanie – regularny przegląd i testowanie oprogramowania, sprzętu, systemów i usług itp. w celu wykrycia słabych punktów systemów wspomagających przetwarzanie;
    - zarządzanie kontrolą dostępu – dostęp do danych osobowych niezbędnych do realizacji zadań związanych z przetwarzaniem danych mają tylko upoważnieni pracownicy, a administrator powinien dokonać zróżnicowania uprawnień dostępu dla upoważnionych pracowników;
        - ograniczenie dostępu (przedstawiciele) – kształtowanie przetwarzania danych powinno przebiegać w taki sposób, aby minimalna liczba osób wymagała dostępu do danych osobowych w celu wykonywania swoich obowiązków; a także odpowiednie ograniczenie dostępu;
        - ograniczenie dostępu (treść) – w przypadku każdej operacji przetwarzania dostęp powinien być ograniczony tylko do tych atrybutów dla danego zbioru danych, które są potrzebne do wykonania tej operacji. Ponadto ograniczenie dostępu do danych osób, których dane dotyczą, podlegających kompetencjom danego pracownika;
        - rozdzielenie dostępu – kształtowanie procesu przetwarzania danych powinno przebiegać w taki sposób, aby żadna osoba nie wymagała pełnego dostępu do

wszystkich danych zebranych na temat osoby, której dane dotyczą, a tym bardziej do wszystkich danych osobowych konkretnej kategorii osób, których dane dotyczą;

- bezpieczne przekazywanie danych – przekazywanie danych powinno być zabezpieczone przed nieuprawnionym i przypadkowym dostępem i wprowadzeniem zmian;
- bezpieczne przechowywanie – przechowywanie danych musi być zabezpieczone przed nieuprawnionym dostępem i wprowadzaniem zmian. Powinny istnieć procedury pozwalające ocenić ryzyko scentralizowanego lub zdecentralizowanego przechowywania oraz kategorie danych osobowych, do których ma to zastosowanie. Niektóre dane mogą wymagać dodatkowych środków bezpieczeństwa lub odizolowania od innych danych;
- pseudonimizację – dane osobowe i kopie zapasowe/rejestry należy spseudonimizować w ramach środków bezpieczeństwa w celu zminimalizowania ryzyka potencjalnych naruszeń ochrony danych, np. przez zastosowanie haszowania lub szyfrowania;
- kopie zapasowe/rejestry – tworzenie kopii zapasowych i prowadzenie rejestrów w zakresie niezbędnym do zapewnienia bezpieczeństwa informacji, wykorzystywanie ścieżek audytu i monitorowanie wydarzeń w ramach rutynowej kontroli bezpieczeństwa. Są one chronione przed nieuprawnionym i przypadkowym dostępem i zmianą oraz regularnie poddawane przeglądowi, a wszelkie zdarzenia powinny być rozpatrywane bezzwłocznie;
- odzyskiwanie danych w przypadku awarii/ciągłość biznesowa – wymagania dotyczące odzyskiwania danych z systemu informacji adresowej w przypadku awarii oraz dotyczące ciągłości biznesowej w celu przywrócenia dostępności danych osobowych po poważnych incydentach;
- ochrona w zależności od ryzyka – wszystkie kategorie danych osobowych powinny być chronione za pomocą środków dostosowanych do ryzyka naruszenia bezpieczeństwa. Dane obarczone szczególnym ryzykiem powinny, w miarę możliwości, być oddzielone od reszty danych osobowych;
- zarządzanie reagowaniem na incydenty naruszające bezpieczeństwo – należy wprowadzić procedury, zasady postępowania i zasoby służące wykrywaniu naruszeń ochrony danych, ograniczaniu naruszeń, postępowaniu z nimi, zgłaszaniu ich i wyciąganiu z nich wniosków;
- zarządzanie incydentami – administrator powinien dysponować procesami umożliwiającymi reagowanie na naruszenia i incydenty, aby system przetwarzania danych był bardziej niezawodny. Dotyczy to również procedur zgłaszania, takich jak zarządzanie zgłoszeniami (do organu nadzorczego) i informacjami (do osób, których dane dotyczą).

Przykład

Administrator chce pobrać duże ilości danych osobowych z medycznej bazy danych zawierającej elektroniczną dokumentację zdrowotną (pacjentów) na dedykowany serwer bazy danych w firmie, aby przetwarzać pobrane dane dla celów związanych z zapewnieniem jakości. Przedsiębiorstwo oceniło ryzyko przekierowania wyciągów na serwer, który jest dostępny dla wszystkich pracowników przedsiębiorstwa, jako prawdopodobnie wysokie dla praw i wolności osób, których dane dotyczą. Ze względu na to, że w firmie istnieje tylko jeden dział, który zajmuje się przetwarzaniem pozyskanych danych pacjentów, administrator danych decyduje się na ograniczenie dostępu do serwera dedykowanego wyłącznie do pracowników tego działu. W celu dalszego zmniejszenia ryzyka, dane przed ich przekazaniem zostaną poddane pseudonimizacji.

Aby uregulować dostęp i zminimalizować ewentualne szkody wynikające ze złośliwego oprogramowania, przedsiębiorstwo postanawia wydzielić sieć i ustanowić środki kontroli dostępu do serwera. Ponadto ustanawia system monitorowania bezpieczeństwa oraz system wykrywania włamań i zapobiegania im, a także wyłącza go z regularnego użytkowania. Wdrożony zostaje zautomatyzowany system kontroli w celu monitorowania dostępu i zmian. W konsekwencji, gdy określone zdarzenia związane z użytkowaniem zostają zaplanowane, generowane są sprawozdania i automatyczne powiadomienia. Administrator zapewnia, aby użytkownicy mieli dostęp tylko na zasadach ściślej potrzeby i z zachowaniem odpowiedniego poziomu dostępu. Niewłaściwe wykorzystanie można szybko i łatwo wykryć.

Konieczne jest porównanie niektórych wyciągów z nowymi wyciągami, a zatem niezbędne jest przechowywanie ich przez trzy miesiące. Administrator decyduje o umieszczeniu ich w oddzielnych bazach danych na tym samym serwerze, a do ich przechowywania stosuje szyfrowanie zarówno transparentne, jak i na poziomie kolumn. Klucze do odszyfrowania danych na poziomie kolumn są przechowywane w dedykowanych modułach bezpieczeństwa, które mogą być używane tylko przez upoważnionych pracowników, jednak nie mogą zostać wyodrębnione.

Postępowanie w przypadku zbliżających się incydentów sprawia, że system jest bardziej solidny i niezawodny. Administrator rozumie, że zapobiegawcze i skuteczne środki i zabezpieczenia powinny stanowić element wszystkich działań w zakresie przetwarzania danych osobowych teraz i w przyszłości oraz że takie działanie może pomóc w zapobieganiu takim naruszeniom ochrony danych w przyszłości.

Administrator ustanawia te środki bezpieczeństwa, aby zapewnić prawidłowość, integralność i poufność, a także aby zapobiec rozprzestrzenianiu się złośliwego oprogramowania w wyniku cyberataków w celu zapewnienia solidnego rozwiązania. Solidne środki bezpieczeństwa przyczyniają się do budowania zaufania wśród osób, których dane dotyczą.

3.9 Rozliczalność[41]

86. Zasada rozliczalności przewiduje, że administrator jest odpowiedzialny za przestrzeganie wszystkich wyżej wymienionych zasad i jest w stanie wykazać ich przestrzeganie.

87. Administrator powinien mieć możliwość wykazania zgodności z tymi zasadami. W ten sposób może on przedstawić skuteczność środków, które zostały podjęte, aby chronić prawa osób, których dane dotyczą, oraz uzasadnić, dlaczego środki te zostały uznane za odpowiednie i skuteczne. Na przykład wykazanie, dlaczego dany środek można uznać za odpowiedni i skuteczny w celu zapewnienia przestrzegania zasady ograniczenia przechowywania.

88. Administrator powinien dysponować zarówno wiedzą na temat ochrony danych, jak i możliwością jej wdrożenia, aby móc odpowiedzialnie przetwarzać dane osobowe. Oznacza to, że administrator danych powinien rozumieć swoje obowiązki w zakresie ochrony danych wynikające z RODO i wywiązywać się z nich.

4 ARTYKUŁ 25 UST. 3 – CERTYFIKACJA

89. Zgodnie z art. 25 ust. 3 certyfikacja na podstawie art. 42 może być stosowana jako element wykazujący zgodność z ochroną danych w fazie projektowania oraz domyślną ochroną danych. Z kolei dokumenty wykazujące zgodność z ochroną danych w fazie projektowania oraz domyślną ochroną danych mogą być również użyteczne w procesie certyfikacji. Oznacza to, że jeżeli operacja przetwarzania przez administratora lub podmiot przetwarzający została poświadczona certyfikatem zgodnie z art. 42, organy nadzorcze uwzględniają to w swojej ocenie zgodności z RODO, w szczególności w odniesieniu do ochrony danych w fazie projektowania oraz domyślnej ochrony danych.

[41] Zob. motyw 74, zgodnie z którym administratorzy są zobowiązani do wykazania skuteczności wprowadzonych przez siebie środków.

90. W przypadku gdy operacja przetwarzania przez administratora lub podmiot przetwarzający jest certyfikowana zgodnie z art. 42, czynnikami, które przyczyniają się do wykazania zgodności z art. 25 ust. 1 i 2, są procesy projektowania, tj. procesy ustalania sposobów przetwarzania, zarządzania oraz środków technicznych i organizacyjnych służących wdrożeniu zasad ochrony danych. Kryteria certyfikacji w zakresie ochrony danych są określane przez podmioty certyfikujące lub właścicieli systemów certyfikacji, a następnie zatwierdzane przez właściwy organ nadzorczy lub przez EROD. Więcej informacji na temat mechanizmów certyfikacji można znaleźć w wytycznych EROD dotyczących certyfikacji[42] oraz innych odpowiednich wytycznych, opublikowanych na stronie internetowej EROD.

91. Nawet w przypadku gdy operacja przetwarzania jest certyfikowana zgodnie z art. 42, administrator nadal jest odpowiedzialny za ciągłe monitorowanie i ulepszanie zgodności z kryteriami ochrony danych w fazie projektowania oraz domyślnej ochrony danych określonymi w art. 25.

5 EGZEKWOWANIE PRZEPISÓW ART. 25 I KONSEKWENCJE

92. Organy nadzorcze mogą przeprowadzić ocenę zgodności z art. 25 zgodnie z procedurami określonymi w art. 58. Uprawnienia naprawcze określono w art. 58 ust. 2 i obejmują one wydawanie ostrzeżeń, udzielanie upomnień, nakazanie poszanowania praw osób, których dane dotyczą, wprowadzenie ograniczenia lub zakazu przetwarzania, zastosowanie administracyjnej kary pieniężnej itp.

93. Ochrona danych w fazie projektowania oraz domyślna ochrony danych są także czynnikiem określającym wysokość sankcji pieniężnych za naruszenie przepisów RODO, zob. art. 83 ust. 4[43] [44].

6 ZALECENIA

94. Wprawdzie art. 25 nie odnosi się bezpośrednio do podmiotów przetwarzających i wytwórców, jednak są oni również uznawani za kluczowe podmioty zapewniające realizację ochrony danych w fazie projektowania oraz domyślnej ochrony danych i powinni zdawać sobie sprawę, że administratorzy danych są zobowiązani do przetwarzania danych osobowych wyłącznie za pomocą systemów i technologii, które mają zintegrowaną ochronę danych.

95. Przetwarzając dane w imieniu administratorów lub dostarczając rozwiązania administratorom danych, podmioty przetwarzające i wytwórcy powinni wykorzystywać swoją wiedzę fachową do budowania zaufania i kierowania działaniami swoich klientów, w tym MŚP, w zakresie projektowania/zapewniania rozwiązań, które włączają ochronę danych do procesów przetwarzania. Oznacza to zaś, że projektowanie produktów i usług powinno wychodzić naprzeciw potrzebom administratorów danych.

96. Wdrażając postanowienia art. 25, należy pamiętać, że głównym celem projektowania jest *skuteczna realizacja* zasad i *ochrona* praw osób, których dane dotyczą, przy zastosowaniu odpowiednich środków przetwarzania. Aby ułatwić i usprawnić przyjęcie ochrony danych w fazie projektowania oraz domyślnej ochrony danych, przekazujemy poniższe zalecenia administratorom, a także wytwórcom i podmiotom przetwarzającym:

- Administratorzy powinni myśleć o ochronie danych już na *początkowych etapach* planowania operacji przetwarzania, nawet przed określeniem sposobów przetwarzania.
- W przypadku gdy administrator danych ma inspektora ochrony danych (IOD), EROD zachęca IOD do aktywnego udziału w procedurach zamówień i rozwoju ochrony danych w fazie projektowania oraz domyślnej ochrony danych, jak również w całym procesie przetwarzania.
- Operacja przetwarzania może być *certyfikowana*. Możliwość uzyskania certyfikacji operacji przetwarzania stanowi wartość dodaną dla administratora danych przy dokonywaniu wyboru między różnymi rodzajami oprogramowania, sprzętu, usług lub systemów przetwarzania pochodzących od wytwórców lub podmiotów przetwarzających. Wytwórcy powinni zatem dążyć do wykazania ochrony danych w fazie projektowania oraz domyślnej ochrony danych w całym procesie opracowywania rozwiązania w zakresie przetwarzania. Pieczęć (znak jakości) certyfikacji może również stanowić dla osób, których dane dotyczą, wskazówkę przy dokonywaniu wyboru między różnymi towarami i usługami. Możliwość uzyskania certyfikacji przetwarzania może służyć jako przewaga konkurencyjna dla wytwórców, podmiotów przetwarzających i administratorów, a nawet zwiększa zaufanie osób, których dane dotyczą, do przetwarzania ich danych osobowych. W przypadku braku certyfikacji administratorzy powinni dążyć do uzyskania innych *form gwarancji* zapewniających, że wytwórcy lub podmioty przetwarzające spełniają wymogi ochrony danych w fazie projektowania oraz domyślnej ochrony danych.
- Administratorzy, podmioty przetwarzające i wytwórcy powinni uwzględnić swoje obowiązki w zakresie zapewnienia dzieciom poniżej 18. roku życia i innym grupom szczególnie wrażliwym szczególnej ochrony w zakresie zgodności z wymogami ochrony danych w fazie projektowania oraz domyślnej ochrony danych.
- Wytwórcy i podmioty przetwarzające powinni dążyć do tego, by ułatwić realizację ochrony danych w fazie projektowania oraz domyślnej ochrony danych w celu wsparcia potencjału administratora w zakresie spełniania obowiązków wynikających z art. 25. Z drugiej strony administratorzy nie powinni wybierać wytwórców lub podmiotów przetwarzających, którzy nie oferują systemów umożliwiających administratorowi spełnienie wymogów art. 25 lub wspierających go w tym procesie, ponieważ administratorzy zostaną pociągnięci do odpowiedzialności za brak ich wdrożenia.
- Wytwórcy i podmioty przetwarzające powinni odgrywać czynną rolę w zapewnieniu spełnienia kryteriów dotyczących „stanu wiedzy technicznej" oraz informować administratorów o wszelkich zmianach „stanu wiedzy technicznej", które mogą wpływać na skuteczność wdrożonych środków. Administratorzy powinni uwzględnić ten wymóg jako klauzulę umowną, aby mieć pewność, że będą informowani na bieżąco.
- EROD zaleca administratorom, aby wymagali od wytwórców i podmiotów przetwarzających wykazania, w jaki sposób ich sprzęt, oprogramowanie, usługi lub systemy umożliwiają administratorowi spełnienie wymogów w zakresie rozliczalności zgodnie z ochroną danych w fazie projektowania oraz domyślną ochrony danych, na przykład poprzez zastosowanie kluczowych wskaźników wydajności w celu wykazania skuteczności środków i zabezpieczeń przy wdrażaniu zasad i praw.
- EROD podkreśla również potrzebę zharmonizowanego podejścia do skutecznego wdrażania zasad i praw oraz zachęca stowarzyszenia lub organy przygotowujące kodeksy postępowania

[42] EROD. „Wytyczne 1/2018 dotyczące certyfikacji i określania kryteriów certyfikacji zgodnie z art. 42 i 43 rozporządzenia". Wersja 3.0, 4 czerwca 2019 r. https://uodo.gov.pl/pl/file/1462

[43] W art. 83 ust. 2 lit. d) RODO stwierdzono, że przy ustalaniu wysokości kar pieniężnych za naruszenie przepisów RODO zwraca się „należytą uwagę" na „stopień odpowiedzialności administratora lub podmiotu przetwarzającego z uwzględnieniem środków technicznych i organizacyjnych wdrożonych przez nich na mocy art. 25 i 32".

[44] Więcej informacji na temat kar pieniężnych znajduje się w wytycznych Grupy Roboczej Art. 29. „Wytyczne w sprawie stosowania i ustalania administracyjnych kar pieniężnych do celów rozporządzenia nr 2016/679". WP 253, 3 października 2017 r. https://uodo.gov.pl/pl/file/21 – zatwierdzone przez EROD

zgodnie z art. 40 do uwzględnienia w nich wytycznych w zakresie ochrony danych w fazie projektowania oraz domyślnej ochrony danych dla poszczególnych sektorów.

- Administratorzy powinni być uczciwi w stosunku do osób, których dane dotyczą, oraz przejrzyści w sposobie oceny i wykazywania skuteczności wdrażania ochrony danych w fazie projektowania oraz domyślnej ochrony danych, podobnie jak administratorzy wykazują zgodność z przepisami RODO w ramach zasady rozliczalności.
- Technologie służące wzmocnieniu ochrony prywatności (PETs), które osiągnęły najwyższy poziom rozwoju, mogą być stosowane jako środek zgodny z wymogami ochrony danych w fazie projektowania oraz domyślnej ochrony danych, w stosownych przypadkach w ramach podejścia opartego na ryzyku. Technologie te nie muszą same w sobie uwzględniać obowiązków wynikających z art. 25. Administratorzy danych oceniają, czy dany środek jest odpowiedni i skuteczny w zakresie wdrażania zasad ochrony danych i praw osób, których dane dotyczą.
- Istniejące dotychczas systemy podlegają tym samym obowiązkom ochrony danych w fazie projektowania oraz domyślnej ochrony danych, co nowe systemy. Jeżeli nie są one już zgodne z wymogami ochrony danych w fazie projektowania oraz domyślnej ochrony danych, a nie można dokonać zmian w celu spełnienia tych wymogów, wówczas przestają spełniać wymogi RODO i nie mogą być dalej wykorzystywane do przetwarzania danych osobowych.
- W art. 25 nie obniżono progu wymogów dla MŚP. Poniższe punkty mogą ułatwić MŚP przestrzeganie przepisów art: 25:
  - przeprowadzanie wczesnych ocen ryzyka
  - wprowadzenie przetwarzania na małej próbie, a następnie rozszerzanie zakresu przetwarzania i stopnia jego zaawansowania
  - oczekiwanie od wytwórcy i pomiotu przetwarzającego gwarancji realizowania ochrony danych w fazie projektowania oraz domyślnej ochrony danych, takich jak certyfikacja i stosowanie kodeksu postępowania
  - korzystanie z pomocy partnerów posiadających dobre wyniki
  - konsultacje z organami ochrony danych
  - zapoznanie się z wytycznymi organów ochrony danych i EROD
  - stosowanie kodeksów postępowania, jeżeli są one dostępne
  - korzystanie z profesjonalnej pomocy i porady.

W imieniu Europejskiej Rady Ochrony Danych

Przewodnicząca

(Andrea Jelinek)



Wytyczne 3/2019 w sprawie przetwarzania danych osobowych przez urządzenia wideo

Wersja 2.0

przyjęta 29 stycznia 2020 r.

Historia wersji

Wersja 2.0	29 stycznia 2020 r.	Przyjęcie wytycznych po konsultacjach publicznych
Wersja 1.0	10 lipca 2019 r.	Przyjęcie wytycznych do konsultacji publicznych

Spis treści

1 Wprowadzenie 5
2 Zakres stosowania 7
2.1 Dane osobowe 7
2.2 Stosowanie dyrektywy 2016/680 7
2.3 Wyjątek domowy i osobisty 8
3 Zgodność przetwarzania z prawem 9
3.1 Prawnie uzasadniony interes, art. 6 ust. 1 lit. f) 9
3.1.1 Istnienie prawnie uzasadnionych interesów 9
3.1.2 Niezbędność przetwarzania 10
3.1.3 Wyważenie interesów 11
3.2 Niezbędność wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi (art. 6 ust. 1 lit. e)) 14
3.3 Zgoda, art. 6 ust. 1 lit. a) 14
4 Ujawnienie nagrań wideo stronom trzecim 16
4.1 Ujawnienie nagrań wideo stronom trzecim – zarys 16
4.2 Ujawnienie nagrań wideo organom ścigania 16
5 Przetwarzanie szczególnych kategorii danych 18
5.1 Względy ogólne dotyczące przetwarzania danych biometrycznych 19
5.2 Proponowane środki minimalizujące ryzyko przy przetwarzaniu danych biometrycznych 22
6 Prawa osoby, której dane dotyczą 24
6.1 Prawo dostępu 24
6.2 Prawo do usunięcia danych i prawo do sprzeciwu 25
6.2.1 Prawo do usunięcia danych (prawo do bycia zapomnianym) 25
6.2.2 Prawo do sprzeciwu 26
7 Przejrzystość i obowiązki informacyjne 28
7.1 Informacje zawarte w pierwszej warstwie (znak ostrzegawczy) 28
7.1.1 Umieszczenie znaku ostrzegawczego 28
7.1.2 Informacje zawarte w pierwszej warstwie 28
7.2 Informacje zawarte w drugiej warstwie 29
8 Okresy przechowywania i obowiązek usunięcia danych 31
9 Środki techniczne i organizacyjne 31
9.1 Przegląd systemu monitoringu wizyjnego 32
9.2 Ochrona danych w fazie projektowania oraz domyślna ochrona danych 33
9.3 Konkretne przykłady odpowiednich środków 34

9.3.1 Środki organizacyjne 34
9.3.2 Środki techniczne 35
10 Ocena skutków dla ochrony danych 37

Europejska Rada Ochrony Danych

uwzględniając art. 70 ust. 1 lit. e) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (zwanego dalej „RODO"),

uwzględniając Porozumienie EOG, a w szczególności jego załącznik XI i protokół 37, w brzmieniu zmienionym decyzją Wspólnego Komitetu EOG nr 154/2018 z dnia 6 lipca 2018 r.[1],

uwzględniając art. 12 i 22 swojego regulaminu wewnętrznego,

PRZYJMUJE NINIEJSZE WYTYCZNE

1 WPROWADZENIE

1. Częste korzystanie z urządzeń wideo wpływa na zachowanie obywateli. Znaczący poziom wdrożenia takich narzędzi w wielu sferach życia osoby wywierać będzie na nią dodatkową presję celem zapobieżenia wykryciu tego, co może być postrzegane jako anomalie. Technologie te mogą *de facto* ograniczać możliwości anonimowego przemieszczania się oraz anonimowego korzystania z usług i generalnie ograniczać możliwość pozostania niezauważonym. Skutki dla ochrony danych są ogromne.
2. Podczas gdy osoby mogą nie mieć nic przeciwko monitoringowi wizyjnemu zainstalowanemu na przykład w określonym celu związanym z bezpieczeństwem, należy ustanowić gwarancje celem uniknięcia niewłaściwego wykorzystywania danych w zupełnie innych i – dla osób, których dane dotyczą – nieoczekiwanych celach (np. w celach marketingowych, monitorowania wydajności pracownika itd.). Ponadto obecnie wdraża się wiele narzędzi służących wykorzystaniu utrwalonych wizerunków i przekształceniu tradycyjnych kamer w inteligentne kamery. Ilość danych generowanych przez nagrania wideo, w połączeniu z tymi narzędziami i technikami, zwiększa ryzyko ich wtórnego wykorzystania (bez względu na to, czy jest ono związane z celem pierwotnie przypisanym systemowi) lub nawet ryzyko związane z niewłaściwym wykorzystaniem danych. Mając do czynienia z monitoringiem wizyjnym, zawsze należy starannie rozważyć ogólne zasady określone w RODO (art. 5).
3. Systemy monitoringu wizyjnego pod wieloma względami zmieniają sposób, w jaki profesjonaliści z sektorów prywatnego i publicznego wchodzą w interakcje w miejscach prywatnych i publicznych w celu zwiększenia bezpieczeństwa, uzyskania analizy publiczności, dostarczenia spersonalizowanych reklam itd. Monitoring wizyjny stał się wysoce skuteczny za sprawą wdrażania na coraz większą skalę inteligentnej analizy obrazu. Techniki te mogą być bardziej (np. złożone technologie biometryczne) lub mniej inwazyjne (np. proste algorytmy liczące). Pozostawanie anonimowym oraz zachowanie prywatności staje się co do zasady coraz trudniejsze. Kwestie związane z ochroną danych podniesione

[1] Odniesienia do „państw członkowskich" w niniejszej opinii należy rozumieć jako odniesienia do „państw członkowskich EOG".

w różnych sytuacjach mogą się różnić, podobnie analiza prawna przy korzystaniu z którejkolwiek z tych technologii.

4. Oprócz kwestii prywatności istnieją również ryzyka związane z ewentualnym nieprawidłowym działaniem tych urządzeń oraz uprzedzeń, które mogą wywoływać. Badacze zauważają, że oprogramowanie wykorzystywane do identyfikacji, rozpoznawania i analizy twarzy działa inaczej w zależności od wieku, płci i pochodzenia etnicznego osoby identyfikowanej. Algorytmy działają w oparciu o zróżnicowane dane demograficzne, w związku z tym stronniczość rozpoznawania twarzy stwarza ryzyko pogłębienia uprzedzeń w społeczeństwie. Dlatego też administratorzy danych muszą również zapewnić, aby przetwarzanie danych biometrycznych, pochodzących z monitoringu wizyjnego, podlegało regularnej ocenie jego istotności i wystarczalności zastosowanych gwarancji.

5. Monitoring wizyjny nie jest domyślnie niezbędny, gdy istnieją inne środki umożliwiające osiągnięcie założonego celu. W przeciwnym razie ryzykujemy zmianę w zakresie norm kulturowych, prowadzącą do zaakceptowania braku prywatności jako warunku startowego.

6. Niniejsze wytyczne mają na celu zapewnienie wskazówek dotyczących stosowania przepisów RODO w związku z przetwarzaniem danych osobowych przez urządzenia wideo. Przedstawione przykłady nie mają charakteru wyczerpującego, ogólny sposób rozumowania można zastosować w odniesieniu do wszystkich potencjalnych obszarów stosowania.

2 ZAKRES STOSOWANIA[2]

2.1 Dane osobowe

7. Systematyczny zautomatyzowany monitoring konkretnego obszaru za pomocą środków optycznych lub audiowizualnych, głównie w celu ochrony mienia lub ochrony życia i zdrowia osoby, stał się znaczącym zjawiskiem naszych czasów. Działanie to wiąże się z gromadzeniem i zatrzymywaniem informacji związanych z obrazem lub audiowizualnych, dotyczących wszystkich osób wchodzących na obszar monitorowany, które można zidentyfikować na podstawie ich wyglądu lub innych cech szczególnych. Szczegóły te często umożliwiają ustalenie tożsamości tych osób. Monitoring umożliwia również dalsze przetwarzanie danych osobowych dotyczących obecności osób i ich zachowania na danym obszarze. Potencjalne ryzyko niewłaściwego wykorzystania danych zwiększa się wraz z wielkością monitorowanego obszaru, jak również z liczbą osób na nim przebywających. Fakt ten znajduje odzwierciedlenie w art. 35 ust. 3 lit. c) RODO, który wymaga przeprowadzenia oceny skutków dla ochrony danych w przypadku systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie, jak również art. 37 ust. 1 lit. b), który wymaga od podmiotów przetwarzających wyznaczenia inspektora ochrony danych w przypadku, gdy operacje przetwarzania, ze względu na swój charakter, wiążą się z regularnym i systematycznym monitorowaniem osób, których dane dotyczą.

8. Rozporządzenie nie ma jednak zastosowania do przetwarzania danych, które nie odnoszą się do konkretnej osoby, np. jeżeli bezpośrednio lub pośrednio nie można zidentyfikować osoby.

> Przykład: RODO nie ma zastosowania do atrap kamer (tj. kamer, które nie funkcjonują jako kamery i w związku z tym nie przetwarzają żadnych danych osobowych). *W niektórych państwach członkowskich kwestia ta może jednak podlegać innym przepisom.*
>
> Przykład: Nagrania wykonane na dużych wysokościach wchodzą w zakres stosowania RODO wyłącznie wtedy, jeżeli w danych okolicznościach przetwarzane dane mogą być powiązane z konkretną osobą.
>
> Przykład: Samochód jest wyposażony w kamerę wideo, która ma pomóc kierowcy w parkowaniu. RODO nie ma zastosowania, jeżeli kamera jest skonstruowana lub dostosowana w taki sposób, że nie gromadzi żadnych informacji dotyczących osoby fizycznej (takich jak numery tablic rejestracyjnych lub informacje, które mogłyby służyć identyfikacji przechodniów).

9.

2.2 Stosowanie dyrektywy 2016/680

10. W zakres stosowania dyrektywy (UE) 2016/680 wchodzi zwłaszcza przetwarzanie danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w tym do celów ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom.

[2] Europejska Rada Ochrony Danych (EROD) zauważa, że – jeżeli i zezwalają na to przepisy RODO – w przepisach krajowych mogą mieć zastosowanie szczególne wymogi.

2.3 Wyjątek domowy i osobisty

11. Zgodnie z art. 2 ust. 2 lit. c) w zakres stosowania RODO nie wchodzi przetwarzanie danych osobowych przez osobę fizyczną w ramach czynności o czysto osobistym lub domowym charakterze[3].

12. W kontekście monitoringu wizyjnego należy przyjąć wąską interpretację niniejszego przepisu – tzw. wyjątku domowego i osobistego. Zatem, jak uznał Trybunał Sprawiedliwości Unii Europejskiej, tzw. „wyjątek domowy i osobisty" powinien być „interpretowany jako obejmujący wyłącznie działania wchodzące w zakres życia prywatnego lub rodzinnego jednostki, co w sposób oczywisty nie ma miejsca w przypadku przetwarzania danych osobowych polegającego na ich opublikowaniu w internecie w taki sposób, że staną się one dostępne dla nieograniczonej liczby osób"[4]. Ponadto jeżeli system monitoringu wizyjnego, w zakresie, w jakim obejmuje on ciągłe nagrywanie i przechowywanie danych osobowych i rozciąga się „choćby częściowo na przestrzeń publiczną i tym samym jest skierowany poza sferę prywatną osoby dokonującej w ten sposób przetwarzania danych, o tyle nie powinien on być rozumiany jako czynność o czysto »osobistym lub domowym charakterze« w rozumieniu art. 3 ust. 2 tiret drugie dyrektywy 95/46"[5].

13. Jeżeli chodzi o urządzenia wideo działające na prywatnej posiadłości danej osoby, mogą one być objęte wyjątkiem domowym i osobistym. Będzie to uzależnione od kilku czynników, które należy w pełni rozważyć, aby wyciągnąć odpowiednie wnioski. Poza wyżej wymienionymi elementami wskazanymi w orzeczeniach TSUE, użytkownik domowego monitoringu wizyjnego musi rozważyć, czy łączą go jakiekolwiek relacje osobiste z osobą, której dane dotyczą, czy skala i częstotliwość monitoringu wskazują na jakąkolwiek działalność zawodową z jego strony, a także potencjalny niekorzystny wpływ monitoringu na osoby, których dane dotyczą. Obecność któregokolwiek z wyżej wymienionych elementów niekoniecznie sugeruje, że przetwarzanie wykracza poza zakres wyjątku domowego i osobistego: aby to stwierdzić, należy dokonać całościowej oceny.

> Przykład: Turysta nagrywa materiał video zarówno telefonem komórkowym, jak i kamerą, aby udokumentować swoje wakacje. Pokazuje nagrania przyjaciołom i rodzinie, lecz nie udostępnia ich nieograniczonej liczbie osób. Taka sytuacja byłaby objęta wyjątkiem domowym i osobistym.
>
> Przykład: Kobieta uprawiająca kolarstwo górskie chce nagrać swój zjazd kamerą sportową. Jeździ ona w odludnym miejscu i zamierza wykorzystać te nagrania wyłącznie do osobistej rozrywki. Taka sytuacja byłaby objęta wyjątkiem domowym i osobistym, nawet jeżeli dane osobowe byłyby w pewnym zakresie przetwarzane.
>
> Przykład: Ktoś monitoruje i nagrywa swój własny ogród. Nieruchomość jest ogrodzona i tylko sam administrator oraz jego rodzina wchodzą do ogrodu regularnie. Taka sytuacja byłaby objęta wyjątkiem domowym i osobistym, pod warunkiem że monitoring wizyjny nie rozciąga się nawet częściowo na przestrzeń publiczną lub sąsiednią nieruchomość.

14.

[3] Zobacz również motyw 18.

[4] Trybunał Sprawiedliwości Unii Europejskiej, wyrok w sprawie C–101/01, Bodil Lindqvist, z dnia 6 listopada 2003 r., pkt 47.

[5] Trybunał Sprawiedliwości Unii Europejskiej, wyrok w sprawie C–212/13, František Ryneš przeciwko Úřad pro ochranu osobních údajů, z dnia 11 grudnia 2014 r., pkt 33.

3 ZGODNOŚĆ PRZETWARZANIA Z PRAWEM

15. Przed rozpoczęciem korzystania z monitoringu wizyjnego należy szczegółowo określić cele przetwarzania (art. 5 ust. 1 lit. b) RODO). Monitoring wizyjny może służyć różnym celom, np. wspieraniu ochrony mienia i majątku, wspieraniu ochrony życia i integralności cielesnej osób, gromadzeniu dowodów przy roszczeniach cywilnych[6]. Te cele monitorowania należy udokumentować na piśmie (art. 5 ust. 2 RODO) i określić w odniesieniu do każdej kamery używanej do monitorowania wizyjnego. Kamery wykorzystywane w tym samym celu przez jednego administratora danych mogą zostać objęte wspólną dokumentacją. Ponadto należy poinformować osoby, których dane dotyczą, o celu lub celach przetwarzania zgodnie z art. 13 (*zob. Rozdział 7, Przejrzystość i obowiązki informacyjne*). Monitoring wizyjny oparty wyłącznie na podstawie, jaką jest cel „bezpieczeństwa" lub „własnego bezpieczeństwa" nie jest pojęciem wystarczająco konkretnym (art. 5 ust. 1 lit. b)). Ponadto jest on sprzeczny z zasadą stanowiącą, że dane osobowe są przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą (zob. art. 5 ust. 1 lit. a)).

16. Co do zasady każda podstawa prawna określona w art. 6 ust. 1 może stanowić podstawę prawną przetwarzania danych pochodzących z monitoringu wizyjnego. Na przykład art. 6 ust. 1 lit. c) ma zastosowanie w przypadku, gdy przepisy krajowe przewidują obowiązek prowadzenia monitoringu wizyjnego[7]. Jednakże w praktyce najprawdopodobniej zostaną zastosowane następujące przepisy:

- art. 6 ust. 1 lit. f) (prawnie uzasadniony interes),
- art. 6 ust. 1 lit. e) (niezbędność wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej).

W wyjątkowych przypadkach art. 6 ust. 1 lit. a) (zgoda) może służyć administratorowi jako podstawa prawna przetwarzania.

3.1 Prawnie uzasadniony interes, art. 6 ust. 1 lit. f)

17. Ocena prawna art. 6 ust. 1 lit. f) powinna opierać się na następujących kryteriach zgodnie z motywem 47.

3.1.1 Istnienie prawnie uzasadnionych interesów

18. Monitoring wizyjny jest zgodny z prawem, o ile jest niezbędny do osiągnięcia celu prawnie uzasadnionego interesu administratora danych lub strony trzeciej, chyba że interesy te są podrzędne wobec interesów osoby, której dane dotyczą, lub podstawowych praw i wolności (art. 6 ust. 1 lit. f)). Prawnie uzasadnione interesy administratora lub strony trzeciej mogą być interesami prawnymi[8], gospodarczymi lub niematerialnymi[9]. Administrator danych powinien jednak wziąć pod uwagę, że jeżeli osoba, której dane dotyczą, wnosi sprzeciw wobec monitorowania zgodnie z art. 21, administrator może prowadzić monitoring wizyjny wobec tej osoby, której dane dotyczą, wyłącznie

[6] Przepisy dotyczące gromadzenia dowodów przy roszczeniach cywilnych różnią się w poszczególnych państwach członkowskich.

[7] Niniejsze wytyczne nie stanowią analizy ni szczegółowego przeglądu przepisów krajowych, które mogą różnić się w poszczególnych państwach członkowskich.

[8] Trybunał Sprawiedliwości Unii Europejskiej, wyrok w sprawie C–13/16, *sprawa Rīgas satiksme*, z dnia 4 maja 2017 r.

[9] Zob. opinię WP 217 Grupy Roboczej Art. 29.

jeżeli stanowi on *ważny* prawnie uzasadniony interes, który jest nadrzędny w stosunku do interesów, praw i wolności osoby, której dane dotyczą, lub w celu ustalenia, dochodzenia i obrony roszczeń.

19. Biorąc pod uwagę realną i niebezpieczną sytuację, cel ochrony nieruchomości przed włamaniem, kradzieżą lub aktami wandalizmu może stanowić prawnie uzasadniony interes dla monitoringu wizyjnego.

20. Prawnie uzasadniony interes musi mieć wymiar realny i stanowić kwestię bieżącą (tj. nie może być fikcyjny lub spekulatywny)[10]. Przed rozpoczęciem monitoringu musi zaistnieć sytuacja rzeczywistego zagrożenia – np. szkody lub poważne incydenty, które miały miejsce w przeszłości. Zgodnie z zasadą rozliczalności, administratorzy powinni dokumentować istotne incydenty (datę, rodzaj, straty finansowe) oraz związane z nimi zarzuty. Takie udokumentowane incydenty mogą stanowić mocne dowody na istnienie prawnie uzasadnionego interesu. Istnienie prawnie uzasadnionego interesu, jak również konieczność monitorowania, powinny podlegać ponownej ocenie w regularnych odstępach czasu (np. raz na rok, w zależności od okoliczności).

> Przykład: Właściciel sklepu chce otworzyć nowy sklep i zainstalować system monitoringu wizyjnego, aby nie dopuścić do aktów wandalizmu. Przedstawiając odpowiednie statystyki może on wykazać, że w najbliższym sąsiedztwie istnieje duże prawdopodobieństwo wystąpienia aktów wandalizmu. Doświadczenia właścicieli sąsiednich sklepów również mogą okazać się przydatne. Administrator, o którym mowa, nie musi ponieść jakichkolwiek szkód. O ile szkody wyrządzone w sąsiedztwie wskazują na wystąpienie jakiegokolwiek niebezpieczeństwa, mogą wskazywać na istnienie prawnie uzasadnionego interesu. Przedstawienie krajowych lub ogólnych statystyk dotyczących przestępczości, bez przeprowadzenia analizy danego obszaru lub zagrożeń dla tego konkretnego sklepu, nie jest jednak wystarczające.

21.

22. Sytuacje stwarzające bezpośrednie zagrożenie mogą stanowić prawnie uzasadniony interes, np. banki lub sklepy zajmujące się sprzedażą cennych towarów (np. biżuterii) lub obszary, które znane są jako typowe miejsca przestępstw przeciwko mieniu (np. stacje paliw).

23. RODO wyraźnie stanowi, że organy publiczne nie mogą przetwarzać danych w oparciu o prawnie uzasadniony interes, dopóki wykonują swoje zadania, art. 6 ust. 1 zdanie 2.

3.1.2 Niezbędność przetwarzania

24. Dane osobowe powinny być adekwatne, stosowne i ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych"), zob. art. 5 ust. 1 lit. c). Przed zainstalowaniem systemu monitoringu wizyjnego administrator powinien zawsze krytycznie ocenić czy środek ten, po pierwsze jest odpowiedni do osiągnięcia pożądanego celu, a po drugie odpowiedni i niezbędny do jego celów. Środki polegające na zastosowaniu monitoringu wizyjnego należy wybierać wyłącznie w przypadku, gdy cel przetwarzania nie mógł zostać osiągnięty w sposób racjonalny za pomocą innych środków, które są mniej inwazyjne w stosunku do podstawowych praw i wolności osoby, której dane dotyczą.

25. Biorąc pod uwagę sytuację, w której administrator chce zapobiec przestępstwom przeciwko mieniu, zamiast instalowania systemu monitoringu wizyjnego administrator mógłby również zastosować alternatywne środki bezpieczeństwa, takie jak ogrodzenie nieruchomości, patrole ochrony, korzystanie

[10] Zob. WP217, Grupa Robocza Art. 29, s. 24 i nn.
Zob. również wyrok TSUE w sprawie C–708/18, s. 44.

z usług strażników, zapewnienie lepszego oświetlenia, zamontowanie zamków, zainstalowanie zabezpieczeń w oknach i drzwiach czy nałożenie powłok lub folii przeciwko graffiti. Środki te mogą być równie skuteczne w zakresie zapobiegania włamaniu, kradzieży i aktom wandalizmu, co systemy monitoringu wizyjnego. Administrator musi ocenić w każdym przypadku z osobna, czy takie środki mogą stanowić racjonalne rozwiązanie.

26. Przed uruchomieniem systemu kamer administrator ma obowiązek ocenić, gdzie i kiedy zastosowanie środków monitoringu wizyjnego jest bezwzględnie konieczne. Zazwyczaj system monitoringu, który działa w porze nocnej, a także poza normalnymi godzinami pracy, sprosta potrzebom administratora w zakresie zapobieżenia ewentualnym zagrożeniom, na które narażona jest jego własność.

27. Ogólnie rzecz biorąc konieczność korzystania z monitoringu wizyjnego w celu ochrony nieruchomości administratorów kończy się na ich granicach.[11] Niemniej istnieją przypadki, w których monitorowanie nieruchomości nie jest wystarczające do zapewnienia skutecznej ochrony. W niektórych indywidualnych przypadkach konieczne może okazać się rozszerzenie zakresu monitoringu wizyjnego, aby objął swoim zasięgiem bezpośrednie otoczenie nieruchomości. W tym kontekście administrator powinien wziąć pod uwagę środki fizyczne i techniczne, na przykład blokowanie obserwacji nieistotnych obszarów lub ich zamazywanie.

> Przykład: Właściciel księgarni chce ją uchronić przed aktami wandalizmu. Co do zasady kamery powinny nagrywać jedynie to, co dzieje się na terenie samych obiektów, ponieważ do tego celu nie jest potrzebne oglądanie sąsiednich nieruchomości lub miejsc dostępnych publicznie, znajdujących się w sąsiedztwie księgarni.

28.

29. Pytania dotyczące niezbędności przetwarzania pojawiają się również w odniesieniu do sposobu przechowywania materiału dowodowego. W niektórych przypadkach niezbędne może być zastosowanie rozwiązań typu „czarnych skrzynek", w przypadku których nagranie jest automatycznie usuwane po upływie określonego okresu przechowywania i dostępne wyłącznie w przypadku wystąpienia incydentu. W innych sytuacjach rejestrowanie materiału wideo może w ogóle nie być konieczne, a bardziej odpowiednim rozwiązaniem byłoby wykorzystanie monitorowania w czasie rzeczywistym. Decyzja między wyborem rozwiązania typu „czarnych skrzynek" a monitoringiem w czasie rzeczywistym powinna być uzależniona od założonego celu. Na przykład jeżeli celem monitoringu wizyjnego jest zabezpieczenie materiału dowodowego, posługiwanie się podglądem w czasie rzeczywistym zazwyczaj nie jest odpowiednie. Monitoring w czasie rzeczywistym może być czasem bardziej inwazyjny niż przechowywanie i automatyczne usuwanie nagrań po upływie określonego terminu (np. jeżeli ktoś nieustannie spogląda na monitor, może to być podejście o wiele bardziej inwazyjne niż w przypadku braku jakiegokolwiek monitora i przechowywania nagrań bezpośrednio w „czarnej skrzynce"). W tym kontekście należy uwzględnić zasadę minimalizacji danych (art. 5 ust. 1 lit. c). Należy również pamiętać, że zamiast korzystania z monitoringu wizyjnego administrator może skorzystać z usług personelu ochrony, który jest w stanie natychmiast zareagować i zainterweniować.

3.1.3 Wyważenie interesów

30. Zakładając, że monitoring wizyjny jest niezbędny do zapewnienia ochrony prawnie uzasadnionych interesów administratora, system monitoringu wizyjnego może zostać wprowadzony do użytku wyłącznie w przypadku, gdy wobec prawnie uzasadnionych interesów administratora lub strony

[11] Taka sytuacja również może podlegać przepisom krajowym w niektórych państwach członkowskich.

trzeciej (np. ochrona mienia lub integralności cielesnej) nadrzędny charakter mają interesy lub podstawowe prawa i wolności osób, których dane dotyczą. Administrator musi uwzględnić 1) w jakim stopniu monitoring wpływa na interesy, podstawowe prawa i wolności osób fizycznych i 2) czy powoduje on naruszenia lub wywołuje negatywne skutki dla praw osób, których dane dotyczą. Wyważanie interesów ma faktycznie charakter obowiązkowy. Z jednej strony należy ocenić i z rozwagą wyważyć podstawowe prawa i wolności, a z drugiej strony prawnie uzasadnione interesy administratora.

Przykład: Prywatna firma parkingowa odnotowała powtarzające się incydenty związane z okradaniem zaparkowanych samochodów. Parking stanowi otwartą przestrzeń i jest łatwo dostępny dla wszystkich, teren ten jest jednak wyraźnie oznaczony znakami i zaporami drogowymi blokującymi przejazd. Firma parkingowa ma prawnie uzasadniony interes (zapobieganie kradzieżom w samochodach klientów) w monitorowaniu obszaru w godzinach, w których jest najbardziej narażona na wystąpienie takich incydentów. Osoby, których dane dotyczą, są monitorowane w określonym czasie, nie przebywają na tym terenie w celach rekreacyjnych, a zapobieganie kradzieżom leży również w ich interesie. Prawnie uzasadniony interes administratora ma w tym przypadku charakter nadrzędny w stosunku do interesu osób, których dane dotyczą, polegający na braku ich monitorowania.

Przykład: Właściciel restauracji postanawia zamontować kamery wideo w toaletach, aby kontrolować stan czystości pomieszczeń sanitarnych. W tym przypadku prawa osób, których dane dotyczą, mają zdecydowanie nadrzędny charakter wobec interesu administratora, a zatem w tym miejscu nie można zamontować kamer.

31.

3.1.3.1 Podejmowanie decyzji w każdym przypadku z osobna

32. W związku z tym, że zgodnie z rozporządzeniem wyważanie interesów ma charakter obowiązkowy, decyzję należy podjąć indywidualnie w każdym przypadku (zob. art. 6 ust. 1 lit. f)). Odnoszenie się do sytuacji abstrakcyjnych lub porównywanie podobnych przypadków jest niewystarczające. Administrator musi ocenić ryzyka związane z naruszeniem praw osób, których dane dotyczą; w tym przypadku decydującym kryterium jest intensywność ingerencji w prawa i wolności osób.

33. Stopień intensywności można określić m.in. w oparciu o rodzaj zgromadzonych informacji (treść informacji), zakres (gęstość informacji, zasięg przestrzenny i geograficzny), liczbę zainteresowanych osób, których dane dotyczą, jako konkretną liczbę lub jako odsetek właściwej populacji, daną sytuację, rzeczywiste interesy grupy osób, których dane dotyczą, środki alternatywne, jak również o charakter i zakres oceny danych.

34. Istotnymi czynnikami równoważącymi mogą być wielkość obszaru objętego monitoringiem oraz liczba osób, których dane dotyczą, objętych monitoringiem. Korzystanie z monitoringu wizyjnego w odludnym miejscu (np. w celu obserwowania zwierząt wolno żyjących lub ochrony infrastruktury krytycznej, takiej jak antena radiowa będąca własnością prywatną) należy oceniać w inny sposób niż monitoring wizyjny wykorzystywany w strefie pieszej lub centrum handlowym.

Przykład: W przypadku zamontowania kamery samochodowej (np. dla celów zgromadzenia dowodów w razie wypadku) należy upewnić się, że kamera ta nie nagrywa w sposób ciągły ruchu drogowego, jak również osób znajdujących się na poboczu. W przeciwnym razie interes posiadania nagrań wideo jako dowodów w razie ewentualnego wypadku drogowego nie może usprawiedliwiać poważnej ingerencji w prawa osób, których dane dotyczą[11].

35.

3.1.3.2 Rozsądne oczekiwania osób, których dane dotyczą

36. Zgodnie z motywem 47 stwierdzenie istnienia prawnie uzasadnionego interesu wymaga przeprowadzenia dokładnej oceny. Należy tu uwzględnić rozsądne oczekiwania osób, których dane dotyczą, podczas i w kontekście przetwarzania ich danych osobowych. Jeżeli chodzi o systematyczne monitorowanie, związek między osobą, której dane dotyczą, a administratorem może być zróżnicowany i wpływać na to, jakie ewentualne rozsądne oczekiwania może mieć osoba, której dane dotyczą. Wykładnia pojęcia „rozsądnych oczekiwań" nie powinna opierać się jedynie na subiektywnych oczekiwaniach. Decydującym kryterium powinno być raczej to, czy obiektywna strona trzecia mogłaby zasadnie oczekiwać i stwierdzić, że została objęta monitoringiem w tej konkretnej sytuacji.

37. Na przykład, w większości przypadków, pracownik nie oczekuje, że będzie monitorowany w swoim miejscu pracy przez pracodawcę[12]. Ponadto nie należy oczekiwać, że monitoring będzie funkcjonował w czyimś prywatnym ogrodzie, w mieszkaniu lub w gabinetach lekarskich i zabiegowych. Z tego samego względu nie jest rozsądne oczekiwanie monitoringu w pomieszczeniach sanitarnych lub saunach – monitorowanie takich pomieszczeń stanowi poważną ingerencję w prawa osób, których dane dotyczą. Rozsądne oczekiwania osób, których dane dotyczą, zakładają że monitoring wizyjny nie zostanie zamontowany w wyżej wymienionych miejscach. Z drugiej strony klient banku może oczekiwać, że jest monitorowany na terenie banku lub w pobliżu bankomatu.

38. Osoby, których dane dotyczą, mogą również oczekiwać, że nie będą monitorowane w miejscach dostępnych publicznie, zwłaszcza jeżeli miejsca te zwykle służą regeneracji, rekonwalescencji i wypoczynkowi, a także w miejscach, w których osoby przebywają lub komunikują się ze sobą, takich jak przestrzenie z wyznaczonymi miejscami do siedzenia, stoliki w restauracjach, parki, kina i centra fitness. W tym przypadku interesy lub prawa i wolności osób, których dane dotyczą, często będą miały nadrzędny charakter w stosunku do prawnie uzasadnionych interesów administratora.

Przykład: Osoby, których dane dotyczą, nie oczekują, że będą monitorowane w toaletach. Monitoring wizyjny używany na przykład w celu zapobieżenia wypadkom nie jest proporcjonalnym środkiem.

39.

40. Znaki informujące osoby, których dane dotyczą, o monitoringu wizyjnym nie są istotne przy określaniu obiektywnych oczekiwań osób, których dane dotyczą. Oznacza to, że np. właściciel sklepu nie może powoływać się na obiektywnie żywione, rozsądne oczekiwania klienta dotyczące monitorowania tylko dlatego, że znak informuje daną osobę o obecności monitoringu już przy wejściu do sklepu.

[12] Zob. także: Grupa Robocza Art. 29, Opinia 2/2017 na temat przetwarzania danych w miejscu pracy, WP 249, przyjęta w dniu 8 czerwca 2017 r.

3.2 Niezbędność wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi (art. 6 ust. 1 lit. e))

41. Dane osobowe mogą być przetwarzane za pośrednictwem monitoringu wizyjnego zgodnie z art. 6 ust. 1 lit. e) jeżeli jest to niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej[13]. Może się okazać, że wykonywanie władzy publicznej nie zezwala na takie przetwarzanie, lecz inne podstawy prawne, takie jak „zdrowie i bezpieczeństwo" dla ochrony odwiedzających i pracowników mogą zapewniać podstawę dla ograniczonego zakresu przetwarzania, przy jednoczesnym uwzględnieniu obowiązków wynikających z RODO i praw osób, których dane dotyczą.

42. Państwa członkowskie mogą utrzymać w mocy lub wprowadzać w życie szczegółowe przepisy krajowe w celu dostosowania zakresu stosowania przepisów RODO dla monitoringu wizyjnego poprzez bardziej precyzyjne określenie szczegółowych wymogów przetwarzania, o ile są one zgodne z zasadami określonymi w RODO (np. ograniczenie przechowywania, proporcjonalność).

3.3 Zgoda, art. 6 ust. 1 lit. a)

43. Zgoda musi zostać wyrażona dobrowolnie, być konkretna, świadoma i jednoznaczna, jak określono w wytycznych dotyczących zgody[14].

44. Jeżeli chodzi o systematyczne monitorowanie, zgoda osoby, której dane dotyczą, może służyć w wyjątkowych przypadkach jako podstawa prawna, jedynie jeżeli jest zgodna z art. 7 (zob. motyw 43). Cechą charakterystyczną monitoringu jest to, że technologia ta monitoruje nieznaną liczbę osób w tym samym czasie. Administratorowi będzie trudno udowodnić, że osoba, której dane dotyczą, wyraziła zgodę przed przetwarzaniem swoich danych osobowych (art. 7 ust. 1). Zakładając, że osoba, której dane dotyczą, wycofa zgodę, administratorowi trudno będzie udowodnić, że jej dane osobowe nie są już przetwarzane (art. 7 ust. 3).

> Przykład: Sportowcy mogą domagać się uruchomienia monitoringu w trakcie ćwiczeń indywidualnych w celu późniejszej analizy swojej techniki i wyników. Z drugiej strony, w przypadku gdy klub sportowy podejmie inicjatywę w zakresie monitorowania całego zespołu w tym samym celu, w większości przypadków zgoda ta nie będzie ważna, gdyż poszczególni sportowcy mogą czuć się zmuszeni do wyrażenia zgody, aby ich odmowa nie wpłynęła negatywnie na kolegów z drużyny.

45.

46. W przypadku gdy administrator zamierza polegać na udzielonej zgodzie, musi zapewnić, aby każda osoba, której dane dotyczą, wchodząca na obszar objęty monitoringiem wizyjnym, wyraziła zgodę na objęcie monitorowaniem. Zgoda ta musi spełniać warunki określone w art. 7. Wejście na oznaczony obszar objęty monitoringiem (np. ludzie zachęcani są do przejścia przez specjalny korytarz lub bramkę, aby wejść na teren objęty monitoringiem) nie stanowi oświadczenia lub jednoznacznej, potwierdzającej czynności, niezbędnych do wyrażenia zgody, chyba że spełnia kryteria z art. 4 i 7, opisane w wytycznych dotyczących zgody[15].

47. Z uwagi na brak równowagi sił między pracodawcami i pracownikami, w większości przypadków pracodawcy nie powinni opierać się na zgodzie przy przetwarzaniu danych osobowych, ponieważ jest mało prawdopodobnym, że zostanie ona udzielona dobrowolnie. W tym kontekście należy wziąć pod uwagę wytyczne dotyczące zgody.

48. W prawie państwa członkowskiego lub w porozumieniach zbiorowych, w tym zakładowych porozumieniach z przedstawicielami pracowników, mogą być przewidziane przepisy szczegółowe o przetwarzaniu danych osobowych pracowników w związku z zatrudnieniem (zob. art. 88).

[13] Podstawa przetwarzania, o którym mowa powyżej, musi być określona w prawie Unii lub państwa członkowskiego i „musi być ono niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi" (art. 6 ust. 3).

[14] Grupa Robocza Art. 29 (GR Art. 29) „Wytyczne dotyczące zgody na mocy rozporządzenia 2016/679" (WP 259 rev.01) – zatwierdzone przez EROD.

[15] Grupa Robocza Art. 29 (GR Art. 29) „Wytyczne dotyczące zgody na mocy rozporządzenia 2016/679" (WP 259) – zatwierdzone przez EROD – które należy wziąć pod uwagę.

4 UJAWNIENIE NAGRAŃ WIDEO STRONOM TRZECIM

49. Co do zasady do ujawniania nagrań wideo stronom trzecim stosuje się przepisy RODO.

4.1 Ujawnienie nagrań wideo stronom trzecim – zarys

50. Pojęcie „ujawniania" zdefiniowano w art. 4 ust. 2 jako przesłanie (np. komunikacja indywidualna), rozpowszechnianie (np. publikowanie w internecie) lub innego rodzaju udostępnianie. Pojęcie „strony trzeciej" zdefiniowano w art. 4 ust. 10. W przypadku ujawnienia danych państwom trzecim lub organizacjom międzynarodowym zastosowanie mają również przepisy szczególne określone w art. 44 i nn.

51. Wszelkie ujawnienie danych osobowych stanowi odrębny rodzaj przetwarzania danych osobowych, dla którego administrator potrzebuje podstawy prawnej określonej w art. 6.

> Przykład: Administrator, który zamierza umieścić nagranie w internecie, musi oprzeć się na podstawie prawnej dla tego przetwarzania, np. uzyskując zgodę osoby, której dane dotyczą, zgodnie z art. 6 ust. 1 lit. a).

52.

53. Nagrania wideo mogą zostać przesłane stronom trzecim w celu innym niż cel, w którym dane osobowe zostały zebrane, na podstawie przepisów art. 6 ust. 4.

> Przykład: Aby umożliwić rozstrzyganie kwestii odszkodowań za ewentualne powstałe szkody, zamontowano monitoring wizyjny rogatki (na parkingu). Powstaje szkoda i nagranie zostaje przesłane prawnikowi w celu zainicjowania sprawy. W tym przypadku cel nagrywania jest taki sam jak cel przesyłania.
>
> Przykład: Aby umożliwić rozstrzyganie kwestii odszkodowań za ewentualne powstałe szkody zamontowano monitoring wizyjny rogatki (na parkingu). Nagranie zostaje opublikowane w internecie wyłącznie w celach rozrywkowych. W tym przypadku cel uległ zmianie i nie jest zgodny z celem pierwotnym. Ponadto określenie podstawy prawnej dla tego przetwarzania (opublikowanie) stanowiłoby problem.

54.

55. Strona trzecia będąca odbiorcą będzie musiała sama przeprowadzić analizę prawną, w szczególności określając na podstawie art. 6 podstawę prawną dla swoich operacji przetwarzania danych (np. przy otrzymywaniu materiałów).

4.2 Ujawnienie nagrań wideo organom ścigania

56. Ujawnienie nagrań wideo organom ścigania jest również niezależnym procesem, wymagającym od administratora odrębnego uzasadnienia.

57. Zgodnie z art. 6 ust. 1 lit. c) przetwarzanie jest zgodne z prawem, jeżeli jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze. Mimo iż obowiązujące prawo dotyczące policji pozostaje pod wyłączną kontrolą państw członkowskich, w każdym państwie członkowskim istnieją zapewne ogólne zasady regulujące przekazywanie materiału dowodowego organom ścigania. Operacje przetwarzania danych przez administratora polegające na przekazywaniu danych są uregulowane przez RODO. W przypadku gdy przepisy krajowe nakładają na administratora obowiązek współpracy z organami ścigania (np. prowadzenia postępowania przygotowawczego), podstawą prawną przekazywania danych jest obowiązek prawny, o którym mowa w art. 6 ust. 1 lit. c).

58. W takim przypadku ograniczenie celu, o którym mowa w art. 6 ust. 4, zazwyczaj nie jest problematyczne, ponieważ ujawnienie wyraźnie odwołuje się do prawa państwa członkowskiego. W związku z tym uwzględnianie szczególnych wymogów w odniesieniu do zmiany celu w kontekście lit. a)–e) nie jest niezbędne.

> Przykład: Właściciel sklepu nagrywa materiał wideo obejmujący wejście do niego. Na nagraniu widać osobę, która kradnie portfel innej osobie. Policja prosi administratora o przekazanie nagrań na potrzeby przeprowadzenia postępowania przygotowawczego. W takim przypadku właściciel sklepu wykorzystałby podstawę prawną, o której mowa w art. 6 ust. 1 lit. c), (obowiązek prawny), czytaną łącznie z odpowiednimi przepisami krajowymi dotyczącymi przetwarzania w postaci przekazywania danych.

59.

> Przykład: Ze względów bezpieczeństwa w sklepie zamontowano kamerę. Właściciel sklepu uważa, że zarejestrował coś podejrzanego, więc postanawia przesłać nagranie policji (bez posiadania informacji o jakimkolwiek prowadzonym postępowaniu przygotowawczym). W tym przypadku właściciel sklepu musi ocenić, czy zostały spełnione warunki, o których mowa (w większości przypadków) w art. 6 ust. 1 lit. f). Jest tak zazwyczaj, gdy właściciel sklepu ma uzasadnione podejrzenie, że doszło do popełnienia przestępstwa.

60.

61. Przetwarzanie danych osobowych przez same organy ścigania nie podlega pod przepisy RODO (zob. art. 2 ust. 2 lit. d)), lecz pod dyrektywę 2016/680.

5 PRZETWARZANIE SZCZEGÓLNYCH KATEGORII DANYCH

62. Systemy monitoringu wizyjnego gromadzą zazwyczaj ogromne ilości danych osobowych, które mogą ujawniać dane o charakterze wysoce osobistym, a nawet szczególne kategorie danych. Pozornie nieistotne dane, zgromadzone za pośrednictwem nagrań wideo, mogą być wykorzystywane do wywnioskowania innych informacji do osiągniecia innego celu (np. mapowania nawyków osób). Monitoring wizyjny nie zawsze jest jednak uznawany za przetwarzający szczególne kategorie danych osobowych.

> Przykład: Nagranie wideo przedstawiające osobę, której dane dotyczą, w okularach lub na wózku inwalidzkim, nie jest samo w sobie uważane za szczególną kategorię danych osobowych.

63.

64. Jeżeli nagranie wideo jest jednak przetwarzane w celu wydedukowania szczególnych kategorii danych, zastosowanie ma art. 9.

> Przykład: Opinie polityczne można na przykład wywnioskować ze zdjęć, na których znajdują się możliwe do zidentyfikowania osoby, których dane dotyczą, uczestniczące w danym wydarzeniu, biorące udział w strajku itd. Taka sytuacja byłaby objęta zakresem stosowania art. 9.
>
> Przykład: Szpital, który zainstalował kamerę wideo w celu monitorowania stanu zdrowia pacjenta, zostałby uznany za przetwarzający szczególne kategorie danych osobowych (art. 9).

65.

66. Co do zasady, w przypadku każdego instalowania systemu monitoringu wizyjnego, należy starannie rozważyć zasadę minimalizacji danych. W związku z tym nawet w przypadkach, w których art. 9 ust. 1 nie ma zastosowania, administrator danych powinien zawsze próbować minimalizować ryzyko utrwalenia nagrania ujawniającego inne dane wrażliwe (wykraczające poza zakres art. 9), niezależnie od celu.

> Przykład: Monitoring wizyjny utrwalający wizerunek kościoła sam w sobie nie jest objęty zakresem art. 9. Administrator musi jednak dokonać wyjątkowo starannej oceny zgodnie z art. 6 ust. 1 lit. f), uwzględniając charakter danych oraz ryzyko utrwalenia innych wrażliwych danych (wykraczających poza zakres art. 9) przy ocenie interesów osób, których dane dotyczą.

67.

68. Jeżeli system monitoringu wizyjnego jest wykorzystywany do przetwarzania szczególnych kategorii danych, administrator danych musi określić zarówno wyjątek dla przetwarzania szczególnych kategorii danych zgodnie z art. 9 (tj. odstępstwo od ogólnej zasady stanowiącej, że nie należy przetwarzać szczególnych kategorii danych) oraz podstawę prawną zgodnie z art. 6.

69. Na przykład art. 9 ust. 2 lit. c) („[…] przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej […]") mógłby – teoretycznie i w wyjątkowych przypadkach – zostać wykorzystany, administrator danych musiałby jednak uzasadnić to bezwzględną niezbędnością zabezpieczenia żywotnych interesów osoby i udowodnić, że ta "[…] osoba, której dane dotyczą, *jest fizycznie lub prawnie niezdolna do wyrażenia zgody*". Ponadto administrator danych nie będzie mógł korzystać z systemu w żadnym innym celu.

70. Należy zauważyć, że nie każde odstępstwo wymienione w art. 9 może być użyte jako uzasadnienie przetwarzania szczególnych kategorii danych za pośrednictwem monitoringu wizyjnego. Konkretniej: administratorzy danych przetwarzający te dane w kontekście monitoringu wizyjnego nie mogą opierać się na art. 9 ust. 2 lit. e), który zezwala na przetwarzanie odnoszące się do danych osobowych w sposób oczywisty upublicznionych przez osobę, której dotyczą. Sam fakt wejścia w zasięg kamery nie oznacza, że osoba, której dane dotyczą, zamierza upublicznić szczególne kategorie danych, które jej dotyczą.

71. Ponadto przetwarzanie szczególnych kategorii danych wymaga wzmożonej i nieustannej czujności w odniesieniu do pewnych obowiązków; na przykład wysokiego poziomu bezpieczeństwa i oceny skutków dla ochrony danych, gdy jest to niezbędne.

> Przykład: Pracodawca nie może wykorzystywać nagrań z monitoringu wizyjnego przedstawiających demonstrację w celu zidentyfikowania strajkujących.

72.

5.1 Względy ogólne dotyczące przetwarzania danych biometrycznych

73. Wykorzystywanie danych biometrycznych, a zwłaszcza technologii rozpoznawania twarzy, wiąże się ze zwiększonymi ryzykami dla praw osób, których dane dotyczą. Kluczowe jest, by korzystanie z takich technologii odbywało się z należytym uwzględnieniem zasad zgodności z prawem, konieczności, proporcjonalności i minimalizacji danych, jak określono w RODO. Podczas gdy używanie takich technologii może być postrzegane jako szczególnie skuteczne, administratorzy powinni jednak najpierw ocenić ich wpływ na podstawowe prawa i wolności oraz rozważyć zastosowanie mniej inwazyjnych środków do osiągnięcia prawnie uzasadnionego celu przetwarzania.

74. Aby dane zostały zakwalifikowane jako dane biometryczne, zgodnie z definicją RODO, przetwarzanie surowych danych, takich jak cechy fizyczne, fizjologiczne lub behawioralne osoby fizycznej, musi zakładać pomiar tych cech. Z uwagi na to, iż dane biometryczne są wynikiem takich pomiarów, art. 4 ust. 14 RODO stanowi, że dane te „[…] wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby […]". Nagranie wideo danej osoby nie może zostać jednak uznane samo w sobie jako zawierające dane biometryczne zgodnie z art. 9, jeżeli nie zostały one specjalnie przetworzone technicznie w celu identyfikacji tej osoby[16].

75. Aby przetwarzanie zostało uznane za przetwarzanie szczególnych kategorii danych osobowych (art. 9), dane biometryczne muszą być przetwarzane „w celu jednoznacznego zidentyfikowania osoby fizycznej".

76. Podsumowując, w świetle art. 4 ust. 14 i art. 9 należy uwzględnić trzy kryteria:

- **Charakter danych:** dane dotyczące cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej,
- **Środki i sposób przetwarzania**: dane, które „wynikają ze specjalnego przetwarzania technicznego",

[16] Motyw 51 RODO wspiera tę analizę stanowiąc, że „[…] Przetwarzanie fotografii nie powinno zawsze stanowić przetwarzania szczególnych kategorii danych osobowych, gdyż fotografie są objęte definicją »danych biometrycznych« tylko w przypadkach, gdy są przetwarzane specjalnymi metodami technicznymi, umożliwiającymi jednoznaczną identyfikację osoby fizycznej lub potwierdzenie jej tożsamości. […]".

- **Cel przetwarzania:** dane muszą być wykorzystane w celu jednoznacznego zidentyfikowania osoby fizycznej.

77. Wykorzystywanie monitoringu wizyjnego, w tym funkcji rozpoznawania biometrycznego, zamontowanego przez podmioty prywatne dla swoich celów (np. w celach marketingowych, statystycznych lub nawet bezpieczeństwa) w większości przypadków będzie wymagało wyraźnej zgody wszystkich osób, których dane dotyczą (art. 9 ust. 2 lit. a)), jednakże zastosowanie może mieć inny odpowiedni wyjątek, o którym mowa w art. 9.

Przykład: Aby udoskonalić swoje usługi spółka prywatna zastępuje punkty identyfikacji pasażerów na lotnisku (punkt nadania bagażu, wejście na pokład) systemami monitoringu wizyjnego, które wykorzystują techniki rozpoznawania twarzy w celu sprawdzenia tożsamości pasażerów, którzy wyrazili zgodę na poddanie się takiej procedurze. Z uwagi na to, że przetwarzanie wchodzi w zakres art. 9, pasażerowie, którzy uprzednio wyraźnie i świadomie wyrazili swoją zgodę, będą musieli się zarejestrować w automatycznym terminalu w celu stworzenia i zarejestrowania „szablonu" twarzy przypisanego do ich karty pokładowej i dowodu tożsamości. Punkty kontroli z funkcją rozpoznawania twarzy muszą być wyraźnie oddzielone, tzn. system należy zainstalować w bramce, aby szablony biometryczne osoby, która nie wyraża na to zgody, nie zostały zarejestrowane. Tylko pasażerowie, którzy uprzednio wyrazili zgodę i kontynuowali rejestrację, skorzystają z bramki wyposażonej w system biometryczny.

Przykład: Administrator zarządza dostępem do swojego budynku przy wykorzystaniu metody rozpoznawania twarzy. Odwiedzający mogą korzystać z tego rodzaju dostępu po uprzednim wyraźnym i świadomym wyrażeniu zgody (zgodnie z art. 9 ust. 2 lit. a)). Niemniej, aby mieć pewność, że nie utrwalono wizerunku żadnej osoby, która uprzednio nie wyraziła na to zgody, metoda rozpoznawania twarzy powinna zostać uruchomiona przez samą osobę, której dane dotyczą, na przykład poprzez wciśnięcie przycisku. Aby zapewnić zgodność przetwarzania z prawem, administrator zawsze musi zaproponować alternatywny sposób uzyskania dostępu do budynku, bez przetwarzania biometrycznego, np. za pomocą identyfikatorów lub kluczy.

78.

79. W tego rodzaju przypadkach, gdy tworzy się szablony biometryczne, administratorzy powinni zapewnić, aby po uzyskaniu wyniku dopasowania lub niedopasowania wszystkie pośrednie szablony wykonane w tle (za wyraźną i świadomą zgodą osoby, której dane dotyczą) w celu porównania ich do tych stworzonych przez osoby, których dane dotyczą, w trakcie rejestracji, zostały niezwłocznie i w bezpieczny sposób usunięte. Szablony stworzone na potrzeby rejestracji powinny być zachowane jedynie do realizacji celu przetwarzania i nie powinny być przechowywane ani archiwizowane.

80. Jeżeli jednak celem przetwarzania jest na przykład odróżnienie jednej kategorii osób od innej, ale nie jednoznaczne zidentyfikowanie danej osoby, wówczas przetwarzanie nie wchodzi w zakres art. 9.

Przykład: Właściciel sklepu chciałby spersonalizować reklamy w oparciu o cechy związane z płcią i wiekiem klienta utrwalone przez system monitoringu wizyjnego. W przypadku gdy system ten nie generuje szablonów biometrycznych w celu jednoznacznego zidentyfikowania osób, a zamiast tego wykrywa jedynie te cechy fizyczne, aby przypisać daną osobę do konkretnej grupy, wówczas przetwarzanie nie wchodzi w zakres art. 9 (o ile nie jest przetwarzany żaden inny rodzaj szczególnych kategorii danych).

81.

82. Art. 9 ma jednak zastosowanie w przypadku gdy administrator przechowuje dane biometryczne (zazwyczaj za pośrednictwem szablonów tworzonych w wyniku wyodrębnienia najważniejszych cech z surowej formy danych biometrycznych (np. wymiarów twarzy ze zdjęcia)), aby jednoznacznie zidentyfikować daną osobę. Jeżeli administrator chce wykryć przypadki ponownego wejścia osoby, której dane dotyczą, na dany obszar lub wejścia na inny obszar (np. w celu dalszego wyświetlania spersonalizowanych reklam), wówczas celem będzie jednoznaczne zidentyfikowanie osoby fizycznej, co oznacza, że od samego początku procedura ta wchodziłaby w zakres art. 9. Tak mogłoby być w przypadku, gdy administrator przechowuje wygenerowane szablony w celu dalszego umieszczania spersonalizowanych reklam na różnych bilbordach w różnych miejscach w sklepie. Z uwagi na to, że system wykorzystuje cechy fizyczne do wykrywania konkretnych osób ponownie wchodzących na obszar objęty zasięgiem kamery (np. osób odwiedzających centrum handlowe) i śledzenia ich, stanowiłoby to metodę identyfikacji biometrycznej, ponieważ ma na celu rozpoznanie z wykorzystaniem specjalnego przetwarzania technicznego.

Przykład: Właściciel sklepu zainstalował system rozpoznawania twarzy na terenie obiektu, aby dopasować swoje reklamy do potrzeb klientów. Administrator danych musi uzyskać wyraźną i świadomą zgodę wszystkich osób, których dane dotyczą, przed wykorzystaniem systemu biometrycznego i dostarczeniem spersonalizowanych reklam. System byłby niezgodny z prawem gdyby utrwalał wizerunek odwiedzających lub przechodniów, którzy nie wyrazili zgody na stworzenie ich szablonów biometrycznych, nawet jeżeli szablon ten zostałby usunięty w możliwie jak najkrótszym czasie. Takie tymczasowe szablony biometryczne rzeczywiście stanowią dane biometryczne przetwarzane w celu jednoznacznego zidentyfikowania osoby, która może nie życzyć sobie otrzymywania spersonalizowanych reklam.

83.

84. EROD zauważa, że niektóre systemy biometryczne są instalowane w środowiskach niekontrolowanych[17], co oznacza, że system obejmuje utrwalanie w tle twarzy wszystkich osób fizycznych znajdujących się w zasięgu kamery, w tym osób, które nie wyraziły zgody na wykorzystanie urządzenia biometrycznego, a zatem na stworzenie szablonów biometrycznych. Szablony te porównuje się do tych stworzonych na potrzeby osób, których dane dotyczą, które uprzednio wyraziły zgodę w trakcie procesu rejestracji (tj. użytkowników urządzeń biometrycznych), aby administrator danych mógł stwierdzić, czy dana osoba jest użytkownikiem urządzeń biometrycznych. W tym przypadku system jest często zaprojektowany w taki sposób, by odróżnić osoby, które chce rozpoznać na podstawie bazy danych od tych, które nie zostały zarejestrowane. Z uwagi na to, że celem jest jednoznaczne zidentyfikowanie osób fizycznych, wyjątek określony w art. 9 ust. 2 RODO jest nadal potrzebny dla każdej osoby, której wizerunek został utrwalony przez kamerę.

[17] Oznacza to, że urządzenie biometryczne mieści się w ogólnodostępnej przestrzeni i może działać w przypadku każdego przechodnia, w przeciwieństwie do systemów biometrycznych w kontrolowanych środowiskach, które mogą być wykorzystywane jedynie przy udziale osoby, która wyraziła zgodę.

Przykład: Hotel korzysta z monitoringu wizyjnego w celu automatycznego powiadomienia menadżera hotelu o przybyciu ważnej osobistości (*ang. VIP*) zaraz po rozpoznaniu wizerunku takiej osoby. Osoby te uprzednio udzieliły wyraźnej zgody na wykorzystywanie funkcji rozpoznawania twarzy przed zarejestrowaniem ich wizerunku w bazie danych utworzonej w tym celu. Te systemy przetwarzania danych biometrycznych byłyby niezgodne z prawem, chyba że wszyscy pozostali goście objęci monitoringiem (w celu zidentyfikowania VIP-ów) wyraziliby zgodę na przetwarzanie zgodnie z art. 9 ust. 2 lit. a) RODO.

Przykład: Administrator instaluje system monitoringu wizyjnego z funkcją rozpoznawania twarzy przy wejściu na salę koncertową, którą zarządza. Administrator musi zapewnić wyraźnie oddzielone wejścia; jedno z systemem biometrycznym i jedno bez takiego systemu (gdzie można zamiast tego np. zeskanować bilet). Wejścia wyposażone w urządzenia biometryczne muszą zostać zbudowane i udostępnione w sposób, który uniemożliwia utrwalanie przez system szablonów biometrycznych widzów, którzy nie wyrazili na to zgody.

85.

86. Wreszcie, w przypadku gdy zgoda jest wymagana na podstawie art. 9 RODO, administrator danych nie powinien uzależniać udzielenia dostępu do swoich usług od zaakceptowania przetwarzania biometrycznego. Innymi słowy, zwłaszcza gdy przetwarzanie biometryczne wykorzystywane jest w celu uwierzytelnienia, administrator danych musi zaproponować alternatywne rozwiązanie, które nie obejmuje przetwarzania biometrycznego – bez ograniczeń lub dodatkowych kosztów dla osoby, której dane dotyczą. Takie alternatywne rozwiązanie jest również niezbędne dla osób, które nie mogą sprostać ograniczeniom urządzenia biometrycznego (niemożność rejestracji lub odczytu danych biometrycznych, trudności z korzystaniem z urządzenia ze względu na niepełnosprawność itd.), zaś w sytuacji, gdy przewiduje się, że korzystanie z urządzenia biometrycznego nie będzie możliwe (np. ze względu na nieprawidłowe działanie), należy przyjąć rozwiązanie "rezerwowe", aby zapewnić ciągłość zaproponowanych usług, ograniczonego jednak do działania w wyjątkowych okolicznościach. W wyjątkowych przypadkach przetwarzanie biometryczne stanowić może główną działalność w ramach usług świadczonych na podstawie umowy, np. muzeum, które organizuje wystawę, aby zaprezentować wykorzystanie urządzenia do rozpoznawania twarzy, w którym to przypadku osoby, których dane dotyczą, nie będą mogły odrzucić przetwarzania danych biometrycznych, gdyby wyraziły chęć wzięcia udziału w wystawie. W takim przypadku zgoda wymagana na podstawie art. 9 nadal jest ważna, jeżeli zostaną spełnione wymogi określone w art. 7.

5.2 Proponowane środki minimalizujące ryzyko przy przetwarzaniu danych biometrycznych

87. Zgodnie z zasadą minimalizacji danych administratorzy danych muszą zapewnić, aby dane pobrane z wizerunku cyfrowego celem stworzenia szablonu nie były nadmierne i zawierały jedynie informacje wymagane w określonym celu, unikając tym samym jakiegokolwiek ewentualnego dalszego przetwarzania. Należy wdrożyć środki w celu zapewnienia, by szablony nie mogły być przesyłane między systemami biometrycznymi.

88. W ramach identyfikacji i uwierzytelniania/weryfikacji najprawdopodobniej niezbędne będzie przechowywanie szablonu w celu jego wykorzystania w późniejszych porównaniach. Administrator danych musi wybrać najbardziej odpowiednie miejsce przechowywania danych. W środowisku kontrolowanym (odgraniczone korytarze lub punkty kontroli) szablony przechowuje się na indywidualnym urządzeniu będącym własnością użytkownika i pozostającym pod jego wyłączną kontrolą (na smartfonie lub w dowodzie tożsamości) lub – gdy są niezbędne do osiągnięcia określonych celów i w przypadku występowania obiektywnych potrzeb – przechowuje się je w scentralizowanej bazie danych w zaszyfrowanej formie, do której klucz dostępu posiada jedynie dana osoba, w celu zapobieżenia nieuprawnionemu dostępowi do szablonu lub miejsca przechowywania. Jeżeli administrator danych nie może zapobiec posiadaniu dostępu do szablonów, musi podjąć odpowiednie kroki, aby zapewnić bezpieczeństwo przechowywanych danych. Może się to wiązać z koniecznością zaszyfrowania szablonu za pomocą algorytmu kryptograficznego.

89. W każdym przypadku administrator podejmuje wszelkie niezbędne środki ostrożności, aby zachować dostępność, integralność i poufność przetwarzanych danych. W tym celu administrator podejmuje przede wszystkim następujące środki: kategoryzuje dane w trakcie ich przesyłania i przechowywania, przechowuje szablony biometryczne i surowe dane lub dane dotyczące tożsamości w odrębnych bazach danych, szyfruje dane biometryczne, zwłaszcza szablony biometryczne i określa politykę w zakresie szyfrowania i zarządzania kluczami kryptograficznymi, wdraża środki organizacyjne i techniczne w zakresie wykrywania oszustw, przypisuje kod uwierzytelniania wiadomości do danych (np. podpis lub skrót) i zapobiega jakiemukolwiek dostępowi do danych biometrycznych z zewnątrz. Takie środki będą musiały być modyfikowane wraz z postępem technologicznym.

90. Poza tym administratorzy danych powinni usunąć surowe dane (wizerunki twarzy, sygnały mowy, sposób chodzenia itd.) i zapewnić, aby takie usunięcie było skuteczne. Jeżeli przestaje istnieć podstawa prawna przetwarzania, należy usunąć surowe dane. O ile szablony biometryczne są tworzone na podstawie takich danych, można rzeczywiście uznać, że utworzenie baz danych mogłoby stanowić równie duże, o ile nie większe, zagrożenie (ponieważ odczytanie szablonu biometrycznego nie zawsze może okazać się łatwym zadaniem bez posiadania wiedzy na temat sposobu, w jaki został on utworzony, podczas gdy surowe dane będą stanowiły elementy niezbędne do utworzenia jakiegokolwiek szablonu). W razie konieczności przechowywania takich danych przez administratora danych, należy rozważyć/zbadać metody addytywne (takie jak dodawanie znaku wodnego), które sprawiłyby, że utworzenie szablonu byłoby nieskuteczne. Administrator musi również usunąć dane i szablony biometryczne w przypadku nieuprawnionego dostępu do terminala służącego porównywaniu odczytów lub serwera przeznaczonego do przechowywania danych oraz usunąć wszystkie dane, które nie są niezbędne do dalszego przetwarzania, pod koniec cyklu życia urządzenia biometrycznego.

6 PRAWA OSOBY, KTÓREJ DANE DOTYCZĄ

91. Z uwagi na charakter przetwarzania danych przy korzystaniu z monitoringu wizyjnego, niektóre prawa osób, których dane dotyczą, przewidziane w RODO muszą zostać dodatkowo objaśnione. Niniejszy rozdział nie ma jednak charakteru wyczerpującego, wszystkie prawa przewidziane w RODO mają zastosowanie do przetwarzania danych osobowych za pośrednictwem monitoringu wizyjnego.

6.1 Prawo dostępu

92. Osoba, której dane dotyczą, ma prawo do uzyskania potwierdzenia ze strony administratora odnośnie do tego, czy jej dane są przetwarzane, czy też nie. W przypadku monitoringu wizyjnego oznacza to, że jeżeli nie przechowuje się ani nie przesyła żadnych danych po zakończeniu okresu, w którym miało miejsce monitorowanie w czasie rzeczywistym, administrator mógłby jedynie przekazać informację o tym, że nie są już przetwarzane żadne dane osobowe (oprócz ogólnych obowiązków informacyjnych, określonych w art. 13, zob. sekcja 7, Przejrzystość i obowiązki informacyjne). Jeżeli w chwili wniesienia żądania dane są jednak nadal przetwarzane (tj. jeżeli dane są przechowywane lub w sposób ciągły przetwarzane w jakikolwiek inny sposób), osoba, której dane dotyczą, powinna uzyskać dostęp i informacje zgodnie z art. 15.

93. Istnieje jednak szereg ograniczeń, które w niektórych przypadkach mogą mieć zastosowanie w związku z prawem dostępu.

- Art. 15 ust. 4 RODO: niekorzystny wpływ na prawa innych osób

94. Z uwagi na fakt, że w tej samej sekwencji monitoringu wizyjnego można zarejestrować dowolną liczbę osób, których dane dotyczą, przegląd nagrania mógłby spowodować dodatkowe przetwarzanie danych osobowych innych osób, których dane dotyczą. Jeżeli osoba, której dane dotyczą, zechce uzyskać kopię nagrań (art. 15 ust. 3) mogłoby to niekorzystnie wpłynąć na prawa i wolności innych osób, których dane dotyczą, których wizerunek został utrwalony na tym nagraniu. Aby temu zapobiec, administrator powinien zatem wziąć pod uwagę fakt, że z uwagi na inwazyjny charakter nagrań wideo administrator w niektórych przypadkach nie powinien przekazywać nagrań wideo, na których można zidentyfikować inne osoby, których dane dotyczą. Ochrona praw stron trzecich nie powinna jednak służyć za wymówkę dla uniemożliwiania osobom zgodnego z prawem dostępu. W takich przypadkach administrator powinien wdrożyć środki techniczne w celu realizacji żądania udzielenia dostępu (na przykład edycja obrazów, m.in. maskowanie lub randomizacja sekwencji bitowych). Administratorzy nie mają jednak obowiązku wdrożenia takich środków technicznych, jeżeli mogą w inny sposób zapewnić swoją gotowość do reagowania na wniosek zgodnie z art. 15, w terminie określonym w art. 12 ust. 3.

- Art. 11 ust. 2: administrator nie jest w stanie zidentyfikować osoby, której dane dotyczą

95. Jeżeli nie da się przeszukać nagrania wideo w celu odnalezienia danych osobowych (tj. administrator musiałby przeszukać znaczną ilość przechowywanych nagrań, aby znaleźć konkretną osobę, której dane dotyczą), administrator może nie być w stanie zidentyfikować osoby, której dane dotyczą.

96. Z tych względów osoba, której dane dotyczą, powinna (oprócz zidentyfikowania się za pomocą dokumentu tożsamości lub osobiście) we wniosku skierowanym do administratora sprecyzować, kiedy – w rozsądnym okresie/przedziale czasowym proporcjonalnym do ilości zarejestrowanych osób, których dane dotyczą – weszła na obszar objęty monitoringiem. Administrator powinien uprzednio powiadomić osobę, której dane dotyczą, o tym, jakie informacje są niezbędne do

zrealizowania wniosku przez administratora. Jeżeli administrator jest w stanie wykazać, że nie ma możliwości zidentyfikowania osoby, której dane dotyczą, administrator musi odpowiednio poinformować o tym osobę, której dane dotyczą, o ile jest to możliwe. W takiej sytuacji, w odpowiedzi udzielonej osobie, której dane dotyczą, administrator powinien zawrzeć informacje na temat konkretnego obszaru objętego monitoringiem, kontroli używanych kamer itd., aby osoba, której dane dotyczą, miała pełną świadomość tego, jakie jej dane osobowe mogły być przetwarzane.

> Przykład: Jeżeli osoba, której dane dotyczą, składa wniosek o uzyskanie kopii swoich danych osobowych, przetwarzanych za pośrednictwem monitoringu wizyjnego przy wejściu do centrum handlowego, które dziennie odwiedza 30 000 osób, osoba, której dane dotyczą, powinna sprecyzować, kiedy znajdowała się na obszarze objętym monitoringiem mniej więcej w godzinowym okienku. Jeżeli administrator nadal przetwarza nagrania, należy dostarczyć kopię nagrania wideo. W przypadku gdy na tym samym nagraniu można zidentyfikować inne osoby, których dane dotyczą, wówczas ten fragment nagrania powinien zostać zanonimizowany (na przykład poprzez zamazanie obrazu kopii nagrania lub jego fragmentu) przed udostępnieniem kopii osobie, której dane dotyczą, która złożyła wniosek.
>
> Przykład: Jeżeli administrator automatycznie usuwa wszystkie nagrania w ciągu na przykład dwóch dni, nie jest on w stanie dostarczyć nagrania osobie, której dane dotyczą, po upływie tego czasu. Jeżeli administrator otrzymuje wniosek po upływie dwóch dni, osoba, której dane dotyczą, powinna zostać o tym odpowiednio poinformowana.

97.

- Art. 12 RODO: nadmierne żądania

98. Jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, administrator może pobrać rozsądną opłatę zgodnie z art. 12 ust. 5 lit. a) RODO lub odmówić podjęcia działań w związku z żądaniem (art. 12 ust. 5 lit. b) RODO). Administrator musi być w stanie wykazać ewidentnie nieuzasadniony lub nadmierny charakter żądania.

6.2 Prawo do usunięcia danych i prawo do sprzeciwu

6.2.1 Prawo do usunięcia danych (prawo do bycia zapomnianym)

99. Jeżeli administrator nadal przetwarza dane osobowe, wykraczając poza monitorowanie w czasie rzeczywistym (np. przechowywanie), osoba, której dane dotyczą, może żądać usunięcia danych osobowych zgodnie z art. 17 RODO.

100. Na żądanie administrator ma obowiązek usunąć bez zbędnej zwłoki dane osobowe, w przypadku wystąpienia jednej z okoliczności wymienionych w art. 17 ust. 1 RODO (i w przypadku gdy nie występuje żaden z wyjątków określonych w art. 17 ust. 3 RODO). Dotyczy to obowiązku usunięcia danych osobowych, które nie są już niezbędne w celu, w którym zostały pierwotnie zebrane lub, w przypadku gdy przetwarzanie jest niezgodne z prawem (zob. również Rozdział 8 – okres przechowywania danych i obowiązek usunięcia danych). Ponadto w zależności od podstawy prawnej przetwarzania dane osobowe powinny zostać usunięte:

- *w przypadku zgody*, gdy zostaje ona wycofana (i nie istnieje żadna inna podstawa prawna przetwarzania),
- *w przypadku prawnie uzasadnionego interesu:*

- gdy tylko osoba, której dane dotyczą, korzysta z prawa do wniesienia sprzeciwu (zob. Rozdział 6.2.2) i nie istnieją żadne nadrzędne ważne, prawnie uzasadnione podstawy przetwarzania, lub
- w przypadku marketingu bezpośredniego (w tym profilowania), kiedy to osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania.

101. W przypadku upublicznienia nagrania wideo przez administratora (np. emisji lub transmisji strumieniowej w internecie na żywo) należy podjąć uzasadnione kroki w celu poinformowania innych administratorów (którzy obecnie przetwarzają dane osobowe) o żądaniu wniesionym zgodnie z art. 17 ust. 2 RODO. Takie uzasadnione kroki powinny obejmować środki techniczne, z uwzględnieniem dostępnych technologii i kosztu ich wdrożenia. W możliwie najszerszym zakresie administrator powinien powiadomić – po usunięciu danych osobowych – wszystkie osoby, którym uprzednio ujawniono dane osobowe, zgodnie z art. 19 RODO.

102. Oprócz obowiązku usunięcia danych osobowych ciążącego na administratorze, na żądanie osoby, której dane dotyczą, administrator jest zobowiązany na mocy ogólnych zasad określonych w RODO do ograniczenia przechowywanych danych osobowych (zob. *Rozdział 8*).

103. W przypadku monitoringu wizyjnego należy zauważyć, że, na przykład poprzez zamazanie obrazu bez możliwości odzyskania danych osobowych znajdujących się uprzednio na obrazie, dane osobowe uważa się za usunięte zgodnie z RODO.

> Przykład: Sklep spożywczy jest narażony na akty wandalizmu, szczególnie jego część zewnętrzna, w związku z czym na zewnątrz przed wejściem, bezpośrednio na ścianach zamontowano monitoring wizyjny. Przechodzień żąda usunięcia swoich danych osobowych utrwalonych na nagraniu w momencie, w którym przechodził obok sklepu. Administrator jest zobowiązany do uwzględnienia żądania bez zbędnej zwłoki i najpóźniej w terminie jednego miesiąca. Z uwagi na to, że dane nagranie nie służy już celowi, w jakim początkowo było przechowywane (nie odnotowano aktów wandalizmu w chwili, gdy osoba, której dane dotyczą, przechodziła obok sklepu), w chwili wniesienia żądania nie istnieje żaden prawnie uzasadniony interes dla przechowywania danych, który miałby nadrzędny charakter wobec interesów osób, których dane dotyczą. Administrator musi usunąć dane osobowe.

104.

6.2.2 Prawo do sprzeciwu

105. W przypadku monitoringu wizyjnego prowadzonego w oparciu o *prawnie uzasadniony interes* (art. 6 ust. 1 lit. f) RODO) lub konieczności przy wykonywaniu zadania w *interesie publicznym* (art. 6 ust. 1 lit. e) RODO) osoba, której dane dotyczą, ma prawo – w dowolnym momencie – do wniesienia sprzeciwu, z przyczyn związanych z jej szczególną sytuacją, wobec przetwarzania zgodnie z art. 21 RODO. Przetwarzanie danych osoby fizycznej musi zostać wstrzymane, chyba że administrator wykaże istnienie ważnych prawnie uzasadnionych podstaw, nadrzędnych wobec praw i interesów osoby, której dane dotyczą. Administrator jest zobowiązany do uwzględnienia żądania osoby, której dane dotyczą, bez zbędnej zwłoki i najpóźniej w terminie jednego miesiąca.

106. W kontekście monitoringu wizyjnego taki sprzeciw można wnieść wchodząc na obszar objęty monitoringiem, w trakcie lub po zakończeniu tego procesu. W praktyce oznacza to, że, o ile administrator nie ma ważnych prawnie uzasadnionych podstaw, monitorowanie danego obszaru, na którym możliwe byłoby zidentyfikowanie osób fizycznych, jest zgodne z prawem jedynie wówczas, gdy

(1) administrator może niezwłocznie zatrzymać przetwarzanie danych osobowych przez kamerę, o ile zgłoszono takie żądanie, lub

(2) dostęp do terenu objętego monitoringiem jest tak ograniczony, że administrator może zapewnić uzyskanie zgody od osoby, której dane dotyczą, przed jej wejściem na dany obszar, do którego osoba, której dane dotyczą, nie ma dostępu jako obywatel.

107. Niniejsze wytyczne nie służą określeniu co jest uznawane za *ważny* prawnie uzasadniony interes (art. 21 RODO).

108. W przypadku korzystania z monitoringu wizyjnego w celach marketingu bezpośredniego, osoba, której dane dotyczą, ma prawo do wniesienia sprzeciwu wobec przetwarzania wedle własnego uznania, ponieważ prawo do sprzeciwu w tym kontekście ma charakter bezwzględny (art. 21 ust. 2 i 3 RODO).

> Przykład: Przedsiębiorstwo mierzy się z problemami dotyczącymi naruszeń bezpieczeństwa przy wejściu na jego teren i korzysta z monitoringu wizyjnego na podstawie prawnie uzasadnionego interesu w celu wychwycenia osób bezprawnie wchodzących na jego teren. Odwiedzający wnosi sprzeciw wobec przetwarzania swoich danych osobowych za pośrednictwem systemu monitoringu wizyjnego z przyczyn związanych z jego szczególną sytuacją. W tym przypadku przedsiębiorstwo nie uwzględnia żądania uzasadniając to faktem, że przechowywane nagranie jest niezbędne ze względu na toczące się dochodzenie wewnętrzne, posiadając tym samym ważne prawnie uzasadnione podstawy do tego, aby kontynuować przetwarzanie danych osobowych.

109.

7 PRZEJRZYSTOŚĆ I OBOWIĄZKI INFORMACYJNE[18]

110. Już od dawna nieodłącznym elementem europejskiego prawa o ochronie danych jest, aby osoby, których dane dotyczą, były świadome faktu działania monitoringu wizyjnego. Osoby te należy szczegółowo informować o miejscach objętych monitoringiem[19]. Zgodnie z RODO ogólne obowiązki w zakresie przejrzystości i obowiązki informacyjne określono w art. 12 RODO i nn. Wytyczne Grupy Roboczej art. 29 w sprawie przejrzystości na mocy rozporządzenia 2016/679 (WP260), które zostały zatwierdzone przez EROD w dniu 25 maja 2018 r., dostarczają dalszych szczegółów. Zgodnie z punktem 26 tychże wytycznych, to art. 13 RODO ma zastosowanie, w przypadku gdy dane osobowe pozyskiwane są „[…] od osoby, której one dotyczą, w drodze obserwacji (np. przy zastosowaniu automatycznych rejestratorów danych lub oprogramowania rejestrującego dane, np. kamer […]".

111. W świetle ilości informacji, które należy dostarczyć osobie, której dane dotyczą, administratorzy danych mogą przyjąć podejście warstwowe, jeżeli zdecydują się na zastosowanie kombinacji metod w celu zapewnienia przejrzystości (WP260, pkt 35; WP89, pkt 22). Odnośnie monitoringu wizyjnego najważniejsze informacje powinny zostać umieszczone na samym znaku ostrzegawczym (pierwsza warstwa), a dalsze obowiązkowe szczegóły mogą być udostępnione za pośrednictwem innych środków (druga warstwa).

7.1 Informacje zawarte w pierwszej warstwie (znak ostrzegawczy)

112. Pierwsza warstwa dotyczy podstawowego sposobu, w jaki administrator po raz pierwszy wchodzi w interakcję z osobą, której dane dotyczą. Na tym etapie administratorzy muszą używać znaku ostrzegawczego przedstawiającego istotne informacje. Przedstawione informacje można opatrzyć znakami graficznymi, które w widoczny, zrozumiały i czytelny sposób przedstawią sens zamierzonego przetwarzania (art. 12 ust. 7 RODO). Format informacji należy dostosować do indywidualnej lokalizacji (WP89 pkt 22).

7.1.1 Umieszczenie znaku ostrzegawczego

113. Informacje należy umieścić w takisposób, aby osoba, której dane dotyczą, mogła z łatwością stwierdzić obecność monitoringu przed wejściem na obszar objęty monitoringiem (mniej więcej na wysokości wzroku). Nie ma konieczności ujawniania miejsca, w którym umieszczono kamerę, o ile nie ma żadnych wątpliwości co do tego, które obszary zostały objęte monitoringiem, a kontekst monitoringu został jednoznacznie wyjaśniony (WP 89, pkt 22). Osoba, której dane dotyczą, musi być w stanie oszacować, który obszar jest obejmowany przez kamerę, aby mogła uniknąć objęcia monitoringiem lub odpowiednio dostosować swoje zachowanie, jeśli zaistnieje taka potrzeba.

7.1.2 Informacje zawarte w pierwszej warstwie

114. Pierwsza warstwa (znak ostrzegawczy) powinna zasadniczo przekazywać najważniejsze informacje, np. szczegóły dotyczące celów przetwarzania, tożsamości administratora i praw przysługujących osobie, której dane dotyczą, oraz najistotniejszych skutków przetwarzania[20]. Może ona obejmować, m.in. prawnie uzasadnione interesy administratora (lub strony trzeciej) oraz dane kontaktowe inspektora ochrony danych (w stosownych przypadkach). Musi się również odnosić do bardziej szczegółowej drugiej warstwy informacji oraz tego, gdzie i w jaki sposób ją znaleźć.

115. Ponadto znak powinien zawierać wszelkie informacje, które mogłyby stanowić zaskoczenie dla osoby, której dane dotyczą (WP260, pkt 38). Może to być na przykład przekazywanie danych stronom trzecim, zwłaszcza jeżeli są one zlokalizowane poza obszarem UE, a także okres przechowywania. W przypadku braku wskazania takich informacji osoba, której dane dotyczą, powinna mieć pewność, że uruchomiony jest tylko monitoring w czasie rzeczywistym (bez rejestrowania danych lub przekazywania danych stronom trzecim).

116.



7.2 Informacje zawarte w drugiej warstwie

117. Drugą warstwę informacyjną również należy udostępnić w miejscu łatwo dostępnym dla osoby, której dane dotyczą, na przykład w formie kompletnego arkusza informacyjnego dostępnego w miejscu centralnym (np. w punkcie informacyjnym, przy recepcji lub przy kasie) lub przedstawić na łatwo dostępnym plakacie. Jak wspomniano powyżej pierwsza warstwa – znak ostrzegawczy – musi wyraźnie odnosić się do drugiej warstwy informacji. Ponadto najlepiej byłoby, jeżeli informacje pierwszej warstwy odnosiły się do źródła cyfrowego (np. kod QR lub adres strony internetowej) drugiej warstwy. Informacje te powinny być jednak łatwo dostępne nie tylko w formie cyfrowej. Powinna istnieć możliwość uzyskania dostępu do informacji drugiej warstwy bez wchodzenia na obszar objęty monitoringiem, zwłaszcza jeżeli informacje zostały udostępnione w formie cyfrowej (można to osiągnąć np. poprzez link). Inne odpowiednie środki mogą objąć numer telefonu, pod który można dzwonić. Bez względu na sposób dostarczenia informacji, muszą one zawierać wszelkie obowiązkowe elementy, o których mowa w art. 13 RODO.

[18] Zastosowanie mogą mieć szczególne wymogi określone w przepisach krajowych.

[19] Zob. WP89, Opinia 4/2004 w sprawie przetwarzania danych osobowych przy nadzorze z użyciem kamer video (Grupa Robocza Art. 29).

[20] Zob. WP260, pkt 38.

118. Oprócz tych opcji, a także by zapewnić większą ich skuteczność, EROD zachęca do korzystania ze środków technicznych w celu dostarczenia informacji osobom, których dane dotyczą. Mogą one obejmować na przykład: kamery geolokalizujące oraz zawieranie informacji w aplikacjach mapowych lub na stronach internetowych, aby osoby mogły z jednej strony z łatwością zidentyfikować i określić źródła wideo, związane z wykonywaniem przysługujących im praw, a z drugiej strony uzyskać bardziej szczegółowe informacje dotyczące procesu przetwarzania.

Przykład: Właściciel sklepu monitoruje swój sklep. Aby spełnić wymogi określone w art. 13, wystarczy przy wejściu do sklepu w widocznym miejscu umieścić znak ostrzegawczy, który zawiera informacje pierwszej warstwy. Ponadto musi on udostępnić arkusz informacyjny zawierający informacje drugiej warstwy przy kasie lub w innym centralnym i łatwo dostępnym miejscu w sklepie.

119.

8 OKRESY PRZECHOWYWANIA I OBOWIĄZEK USUNIĘCIA DANYCH

120. Danych osobowych nie można przechowywać przez okres dłuższy niż jest to niezbędne do celów, w których dane te są przetwarzane (art. 5 ust. 1 lit. c) i e) RODO). W niektórych państwach członkowskich mogą istnieć przepisy szczegółowe dotyczące okresów przechowywania w związku z monitoringiem wizyjnym, zgodnie z art. 6 ust. 2 RODO.

121. To, czy istnieje konieczność przechowywania danych, czy też nie, powinno podlegać kontroli w krótkim okresie. Co do zasady prawnie uzasadnione cele prowadzenia monitoringu wizyjnego to często ochrona mienia lub zabezpieczenie materiału dowodowego. Powstałe szkody można zazwyczaj stwierdzić w ciągu jednego lub dwóch dni. Aby umożliwić wykazanie zgodności z ramami prawnymi ochrony danych, w interesie administratora leży dokonanie uprzednich ustaleń organizacyjnych (np. wyznaczenie, w stosownych przypadkach, osoby odpowiedzialnej za przegląd i zabezpieczenie nagrań wideo). Uwzględniając zasady określone w art. 5 ust. 1 lit. c) i e) RODO, a mianowicie minimalizacji danych i ograniczenia przechowywania, w większości przypadków (np. dla celu wykrycia aktów wandalizmu) dane osobowe powinny zostać usunięte, najlepiej automatycznie, po kilku dniach. Im dłuższy okres przechowywania (zwłaszcza, gdy przekracza on 72 godziny), tym więcej należy przedstawić argumentów przemawiających za zgodnością z prawem celu i konieczności przechowywania. W przypadku gdy administrator korzysta z monitoringu wizyjnego nie tylko w celu monitorowania swojej nieruchomości, lecz zamierza również przechowywać dane, administrator musi zapewnić, aby przechowywanie to było rzeczywiście niezbędne do osiągnięcia założonego celu. W takim przypadku należy wyraźnie wskazać okres przechowywania i określić go indywidualnie dla każdego celu. Do obowiązków administratora należy określenie okresu przechowywania zgodnie z zasadami konieczności (niezbędności) i proporcjonalności, a także wykazanie zgodności z przepisami RODO.

Przykład: Właściciel małego sklepu zapewne zauważyłby wszelkie akty wandalizmu już w dniu, w którym ich dokonano. A zatem normalny okres przechowywania wynoszący 24 godziny jest wystarczająco długi. Weekendy i dni wolne od pracy mogłyby jednak przemawiać za dłuższym okresem przechowywania. W przypadku wykrycia jakichkolwiek szkód właściciel prawdopodobnie będzie musiał przechowywać nagranie wideo przez dłuższy okres, w celu wszczęcia postępowania przeciwko sprawcy przestępstwa.

122.

9 ŚRODKI TECHNICZNE I ORGANIZACYJNE

123. Jak określono w art 32 ust. 1 RODO, przetwarzanie danych osobowych w trakcie działania monitoringu wizyjnego musi być nie tylko dozwolone z prawnego punktu widzenia, lecz także administratorzy i podmioty przetwarzające muszą je odpowiednio zabezpieczyć. Wdrożone **środki techniczne i organizacyjne** muszą być **proporcjonalne do zagrożeń stwarzanych wobec praw i wolności osób fizycznych**, wynikających z przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych pochodzących z monitoringu wizyjnego. Zgodnie z art. 24 i art. 25 RODO administratorzy muszą wdrożyć środki techniczne i organizacyjne, aby zapewnić stosowanie wszelkich zasad dotyczących ochrony danych w trakcie ich przetwarzania i ustanowić środki dla osób, których dane dotyczą, umożliwiające wykonywanie ich praw, o których mowa w art. 15–22 RODO. Administratorzy danych powinni przyjąć wewnętrzne ramy i polityki, aby zapewnić takie wdrażanie zarówno w chwili określania

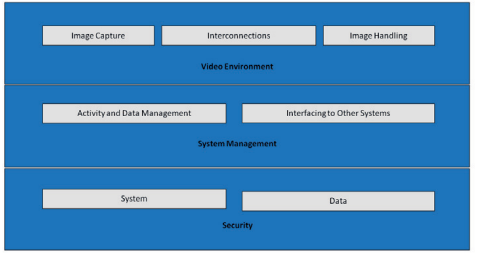
środków przetwarzania, jaki w czasie samego przetwarzania, w tym przeprowadzenia oceny skutków dla ochrony danych, w razie potrzeby.

9.1 Przegląd systemu monitoringu wizyjnego

124. Na system monitoringu wizyjnego (SMW)[21] składają się urządzenia analogowe i cyfrowe, jak również oprogramowanie służące utrwalaniu obrazów, ich przetwarzaniu i wyświetlaniu operatorowi. Jego składniki zostały pogrupowane w następujące kategorie:

- Środowisko wizualne: utrwalanie obrazu, wzajemne połączenia i przetwarzanie obrazów;
  - celem utrwalania obrazu jest tworzenie obrazu otaczającej rzeczywistości w takim formacie, który może zostać wykorzystany przez pozostałe funkcje systemu,
  - wzajemne połączenia odnoszą się do wszystkich środków przesyłania danych w obrębie środowiska wizualnego, tj. łącza i komunikacja. Przykładami łączy są kable, sieci cyfrowe i transmisje bezprzewodowe. Komunikacja odnosi się do wszystkich sygnałów danych wideo i danych kontrolnych, które mogą być cyfrowe lub analogowe,
  - przetwarzanie obrazów obejmuje analizę, przechowywanie i prezentację obrazu lub sekwencji obrazów.
- Z perspektywy zarządzania systemem, SMW posiada następujące funkcje logiczne:
  - zarządzanie danymi i zarządzanie działaniami, które obejmują obsługę poleceń operatora oraz działania generowane przez system (procedury alarmowe, podmioty alarmujące),
  - interfejsy innych systemów mogą obejmować połączenia z innymi systemami bezpieczeństwa (kontrola dostępu, alarm pożarowy) oraz systemami niezwiązanymi z bezpieczeństwem (tworzenie systemów zarządzania, automatyczne rozpoznawanie tablic rejestracyjnych).
- Na bezpieczeństwo SMW składa się poufność, integralność i dostępność systemu i danych:
  - bezpieczeństwo systemu obejmuje bezpieczeństwo fizyczne wszystkich elementów systemu i kontrolę dostępu do SMW,
  - bezpieczeństwo danych obejmuje zapobieganie utracie lub manipulacji danych.

[21] RODO nie zawiera żadnej definicji, techniczny opis można zaleźć, na przykład w EN 62676-1-1:2014 Systemy dozorowe CCTV stosowane w zabezpieczeniach – część 1–1: Wymogi dotyczące systemu wideo.



125.

Image Capture	Utrwalanie obrazu
Interconnections	Wzajemne połączenia
Image Handling	Przetwarzanie obrazów
Video Environment	Środowisko wizualne
Activity and Data Management	Zarządzanie działaniami i danymi
Interfacing to Other Systems	Połączenia z innymi systemami
System Management	Zarządzanie systemem
System	System
Data	Dane
Security	Bezpieczeństwo

Rys. 1 – system monitoringu wizyjnego

9.2 Ochrona danych w fazie projektowania oraz domyślna ochrona danych

126. Jak określono w art. 25 RODO, administratorzy muszą wdrożyć odpowiednie środki techniczne i organizacyjne w zakresie ochrony danych już w fazie planowania monitoringu wizyjnego – przed rozpoczęciem gromadzenia i przetwarzania nagrań wideo. Zasady te podkreślają potrzebę wbudowanych technologii służących wzmocnieniu ochrony prywatności, ustawień domyślnych, które minimalizują przetwarzanie danych, oraz zapewnienia niezbędnych narzędzi umożliwiających jak najlepszą ochronę danych osobowych[22].

127. Administratorzy powinni tworzyć zabezpieczenia służące ochronie danych i prywatności nie tylko w ramach specyfikacji technicznych projektu, lecz również praktyk organizacyjnych. Jeżeli chodzi o praktyki organizacyjne, administrator powinien przyjąć odpowiednie ramy zarządzania, ustanowić i realizować polityki i procedury dotyczące monitoringu wizyjnego. Z technicznego punktu widzenia specyfikacja i projekt systemu powinny obejmować wymogi w zakresie przetwarzania danych osobowych zgodnie z zasadami określonymi w art. 5 RODO (zgodność przetwarzania z prawem, ograniczenie celu i danych, domyślna minimalizacja danych w rozumieniu art. 25 ust. 2 RODO,

[22] Opinia WP 168 w sprawie „Przyszłości prywatności", wspólny wkład Grupy Roboczej Art. 29 i Grupy Roboczej ds. Policji i Wymiaru Sprawiedliwości do Konsultacji Komisji Europejskiej w sprawie ram prawnych dla podstawowego prawa do ochrony danych osobowych (przyjęta w dniu 1 grudnia 2009 r.).

integralność i poufność danych, rozliczalność itd.). W przypadku gdy administrator planuje nabyć komercyjny system monitoringu wizyjnego, musi on zawrzeć te wymogi w specyfikacji zakupu. Administrator musi zapewnić zgodność z tymi wymogami, stosując je w odniesieniu do wszystkich elementów składowych systemu i do wszystkich danych przetwarzanych w ramach tego systemu w trakcie całego cyklu ich życia.

9.3 Konkretne przykłady odpowiednich środków

128. Większość środków, które mogą służyć zabezpieczeniu monitoringu wizyjnego, zwłaszcza w przypadku wykorzystania sprzętu i oprogramowania cyfrowego, nie będzie się różnić od tych, które zostały wykorzystane w innych systemach informatycznych. Niemniej, bez względu na wybrane rozwiązanie, administrator musi odpowiednio chronić wszystkie składniki systemu monitoringu wizyjnego oraz dane na wszystkich etapach, tj. w trakcie przechowywania (dane nieaktywne), przesyłania (dane przesyłane) i przetwarzania (dane wykorzystywane). W tym celu niezbędne jest, by administratorzy i podmioty przetwarzające łączyli środki techniczne i organizacyjne.

129. Przy wyborze rozwiązań technicznych administrator powinien rozważyć wprowadzenie technologii chroniących prywatność, również dlatego że zwiększają one bezpieczeństwo. Przykładami takich technologii są systemy umożliwiające maskowanie lub randomizację sekwencji bitowych obszarów, które pozostają bez znaczenia dla monitoringu, a także usunięcie wizerunku osób trzecich przed dostarczeniem nagrania wideo osobom, których dane dotyczą[23]. Z drugiej strony wybrane rozwiązania nie powinny zawierać funkcji, które nie są niezbędne (np. nieograniczone ruchy kamery, możliwość przybliżenia, transmisja radiowa, analiza i nagrania dźwiękowe). Funkcje, które są dostępne i nie są niezbędne, należy dezaktywować.

130. Istnieje wiele materiałów na ten temat, w tym międzynarodowe normy i specyfikacje techniczne w zakresie bezpieczeństwa fizycznego systemów multimedialnych[24] oraz ogólnego bezpieczeństwa systemów informatycznych[25]. W związku z tym sekcja ta zawiera jedynie przegląd kluczowych zagadnień dotyczących tego tematu.

9.3.1 Środki organizacyjne

131. Oprócz potencjalnie niezbędnej oceny skutków dla ochrony danych (zob. Rozdział 10) administratorzy powinni wziąć pod uwagę następujące wątki przy tworzeniu swoich polityk i procedur w zakresie monitoringu wizyjnego:

- Kto odpowiada za zarządzanie i obsługę systemu monitoringu wizyjnego.
- Cel i zakres projektu monitoringu wizyjnego.
- Właściwe i niedozwolone wykorzystanie (w jakich miejscach i w jakim czasie wykorzystanie monitoringu wizyjnego jest dozwolone, a kiedy i gdzie nie jest; np. wykorzystanie ukrytych kamer i nagrań dźwiękowych oprócz nagrań wideo)[26].

[23] W niektórych przypadkach wykorzystanie takich technologii może być obowiązkowe w celu spełnienia wymogów, o których mowa w art. 5 ust. 1 lit. c). W każdym razie mogą one posłużyć jako przykłady najlepszych praktyk.

[24] IEC TS 62045 – Bezpieczeństwo multimedialne – Wskazówki dotyczące ochrony prywatności używanego i nieużywanego sprzętu oraz systemów.

[25] ISO/IEC 27000 – Seria „Systemy zarządzania bezpieczeństwem informacji".

[26] Może to być uzależnione od przepisów krajowych i regulacji dotyczących danego sektora.

- Środki służące przejrzystości, o których mowa w Rozdziale 7 (*Przejrzystość i obowiązki informacyjne*).
- W jaki sposób rejestruje się nagrania wideo i na jaki czas, uwzględniając okres archiwizacji nagrań wideo związany z incydentami bezpieczeństwa.
- Kto musi przejść odpowiednie szkolenie i kiedy.
- Kto ma dostęp do nagrań wideo i w jakich celach.
- Procedury operacyjne (np. kto i z jakiego miejsca sprawuje nadzór nad monitoringiem wizyjnym, jak postępować w przypadku naruszenia ochrony danych).
- Do jakich procedur wnioskowania o uzyskanie dostępu do nagrań wideo muszą stosować się strony zewnętrzne oraz procedury dotyczące odrzucenia lub uznania wniosku.
- Procedury dotyczące zamówienia, instalacji i konserwacji SMW.
- Procedury zarządzania incydentami oraz odzyskiwania danych.

9.3.2 Środki techniczne

132. **Bezpieczeństwo systemu** oznacza **bezpieczeństwo fizyczne** wszystkich elementów składowych systemu i integralność systemu, tj. **ochronę przed umyślną i nieumyślną ingerencją w normalne działania systemu i odporność na nią** oraz **kontrolę dostępu**. Bezpieczeństwo danych oznacza **poufność** (dane są dostępne wyłącznie dla osób, którym przyznano dostęp), **integralność** (zapobieganie utracie lub manipulowaniu danych) oraz **dostępność** (można uzyskać dostęp do danych, gdy jest to wymagane).

133. **Bezpieczeństwo fizyczne** stanowi istotny element ochrony danych oraz pierwszą linię obrony, ponieważ zapobiega przed kradzieżą sprzętu SMW, aktami wandalizmu, klęskami żywiołowymi, katastrofami spowodowanymi przez człowieka i przypadkowymi uszkodzeniami (np. w wyniku przepięcia, ekstremalnych temperatur, czy też rozlanej kawy). W przypadku systemu analogowego bezpieczeństwo fizyczne odgrywa główną rolę w zapewnieniu ich ochrony.

134. **Bezpieczeństwo systemu i danych**, tzn. ochrona przed umyślną i nieumyślną ingerencją w jego normalne działania, może obejmować:

- ochronę całej infrastruktury SMW (w tym kamery zdalnie sterowane, okablowanie i zasilanie) przed fizyczną ingerencją i kradzieżą,
- ochronę przesyłania nagrań wideo za pośrednictwem kanałów komunikacyjnych zabezpieczonych przed przechwytywaniem danych,
- szyfrowanie danych,
- korzystanie z rozwiązań opartych na wykorzystaniu sprzętu i oprogramowania, takich jak zapory sieciowe, systemy antywirusowe i systemy wykrywania włamań, chroniące przed cyberatakami,
- wykrywanie awarii elementów składowych, oprogramowania i wzajemnych połączeń,
- środki służące odzyskiwaniu dostępności i dostępu do systemu w razie incydentu fizycznego lub technicznego.

135. **Kontrola dostępu** gwarantuje, że tylko osoby upoważnione będą miały dostęp do systemu i danych, podczas gdy pozostałe osoby są takiej możliwości pozbawione. Środki wspierające kontrolę dostępu fizycznego i logicznego obejmują:

- Zapewnienie zabezpieczenia wszystkich obiektów objętych monitoringiem wizyjnym i w których przechowywane są nagrania wideo, przed niekontrolowanym dostępem przez strony trzecie.

- Ustawienie monitorów w taki sposób (zwłaszcza jeżeli znajdują się one w przestrzeniach otwartych, takich jak recepcja), aby ich ekrany mogły być widoczne jedynie dla upoważnionych operatorów.
- Określono i wdrożono procedury w zakresie przyznania, zmiany i wycofania dostępu fizycznego i logicznego.
- Wdrożono metody i środki uwierzytelniania i autoryzacji użytkowników, obejmujące m.in. długość haseł i częstotliwość ich zmiany.
- Działania użytkowników (zarówno w odniesieniu do systemu, jak i danych) są rejestrowane i poddawane regularnym przeglądom.
- Problemy z dostępem są na bieżąco monitorowane i identyfikowane, a wykryte podatności są rozwiązywane możliwie jak najszybciej.

10 OCENA SKUTKÓW DLA OCHRONY DANYCH

136. Zgodnie z art. 35 ust. 1 RODO administratorzy są zobowiązani do przeprowadzenia oceny skutków dla ochrony danych (DPIA), w przypadku gdy dany rodzaj przetwarzania danych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Art. 35 ust. 3 lit. c) RODO stanowi, że administratorzy mają obowiązek przeprowadzenia ocen skutków dla ochrony danych, jeżeli przetwarzanie stanowi systematyczne monitorowanie miejsca dostępnego publicznie na dużą skalę. Ponadto zgodnie z art. 35 ust. 3 lit. b) RODO należy również przeprowadzić ocenę skutków dla ochrony danych, w przypadku gdy administrator zamierza przetwarzać szczególne kategorie danych na dużą skalę.

137. Wytyczne dotyczące oceny skutków dla ochrony danych[27] zawierają dalsze wskazówki i bardziej szczegółowe przykłady odnoszące się do monitoringu wizyjnego (np. dotyczące „wykorzystywania systemu kamer w celu monitorowania zachowania kierowców na autostradach"). Zgodnie z art. 35 ust. 4 RODO wszystkie organy nadzorcze są zobowiązane do opublikowania wykazu rodzaju operacji przetwarzania podlegających obowiązkowemu przeprowadzeniu oceny skutków dla ochrony danych (DPIA) w ich państwie. Wykazy te można zwykle znaleźć na stronach internetowych organów. Biorąc pod uwagę typowe cele monitoringu wizyjnego (ochrona osób i mienia, wykrywanie przestępstw, zapobieganiem im oraz ich kontrola, gromadzenie materiału dowodowego i identyfikacja biometryczna podejrzanych), zasadne jest założenie, że w wielu przypadkach dotyczących monitoringu wizyjnego konieczne będzie przeprowadzenie oceny skutków dla ochrony danych. Dlatego też administratorzy danych powinni uważnie zapoznać się z tymi dokumentami, aby stwierdzić, czy istnieje konieczność przeprowadzenia takiej oceny i przeprowadzić ją, jeśli to niezbędne. Wybór administratora w zakresie wdrażanych środków ochrony danych powinien być podyktowany wynikiem przeprowadzonej oceny skutków dla ochrony danych.

138. Należy również zauważyć, że jeśli wyniki oceny skutków dla ochrony danych wskazują, że przetwarzanie stanowiłoby wysokie ryzyko pomimo planowanego wdrożenia środków bezpieczeństwa przez administratora, wówczas konieczne będzie skonsultowanie się z odpowiednim organem nadzorczym przed rozpoczęciem przetwarzania. Szczegóły dotyczące uprzednich konsultacji można znaleźć w art. 36.

W imieniu Europejskiej Rady Ochrony Danych

Przewodnicząca

(Andrea Jelinek)

[27] WP248 rev.01, Wytyczne dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko", do celów rozporządzenia 2016/679. – zatwierdzone przez EROD



Wytyczne 2/2019 w sprawie przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. b) rozporządzenia w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (RODO) w kontekście świadczenia usług online na rzecz osób, których dane dotyczą

Wersja 2.0

8 października 2019 r.

Historia wersji

Wersja 2.0	8 października 2019 r.	Przyjęcie wytycznych po konsultacjach publicznych
Wersja 1.0	9 kwietnia 2019 r.	Przyjęcie wytycznych do konsultacji publicznych

1 Część I Wprowadzenie 4
1.1 Kontekst 4
1.2 Zakres stosowania wytycznych 5
2 Część 2 – Analiza art. 6 ust. 1 lit. b) 6
2.1 Uwagi ogólne 6
2.2 Interakcja treści art. 6 ust. 1 lit. b) z pozostałymi podstawami prawnymi przetwarzania 7
2.3 Zakres zastosowania art. 6 ust. 1 lit. b) 8
2.4 Niezbędność 8
2.5 Niezbędne do wykonania umowy zawartej z osobą, której dane dotyczą 9
2.6 Rozwiązanie umowy 12
2.7 Niezbędne do podjęcia działań przed zawarciem umowy 13
3 Część 3 – Stosowanie art. 6 ust. 1 lit. b) w określonych sytuacjach 14
3.1 Przetwarzanie w celu „poprawy jakości usługi" 14
3.2 Przetwarzanie w celu „zapobiegania oszustwom" 15
3.3 Przetwarzanie na potrzeby internetowej reklamy behawioralnej 15
3.4 Przetwarzanie w celu personalizacji treści 16

Europejska Rada Ochrony Danych

uwzględniając art. 70 ust. 1 lit. e) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE,

PRZYJMUJE NINIEJSZE WYTYCZNE:

1 CZĘŚĆ I WPROWADZENIE

1.1 Kontekst

1. Zgodnie z art. 8 Karty praw podstawowych Unii Europejskiej dane osobowe muszą być przetwarzane rzetelnie w określonych celach i na uzasadnionej podstawie przewidzianej ustawą. W tym względzie art. 6 ust. 1 ogólnego rozporządzenia o ochronie danych (RODO)[1] stanowi, że przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy spełniony jest co najmniej jeden z sześciu warunków określonych w art. 6 ust. 1 lit. a–f. Określenie właściwej podstawy prawnej, która odpowiada celowi i istocie przetwarzania ma zasadnicze znaczenie. Administratorzy danych uwzględniają, między innymi, wpływ na prawa osób, których dane dotyczą, przy określaniu właściwej podstawy prawnej w celu poszanowania zasady rzetelności.

2. Artykuł 6 ust. 1 lit. b) RODO stanowi podstawę prawną przetwarzania danych w zakresie, w jakim „przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy"[2]. Wspiera to swobodę prowadzenia działalności gospodarczej zagwarantowaną w art. 16 Karty i odzwierciedla fakt, że czasami zobowiązań umownych wobec osoby, której dane dotyczą, nie można wykonać bez przekazania przez osobę, której dane dotyczą, pewnych danych osobowych. Jeżeli określone przetwarzanie jest nieodłączną częścią świadczonej usługi, w interesie obu stron leży przetwarzanie tych danych, ponieważ w przeciwnym razie usługa nie mogłaby zostać zrealizowana, a umowa nie mogłaby zostać zawarta ani wykonana. Możliwość korzystania z tej lub jednej z pozostałych podstaw prawnych, o których mowa w art. 6 ust. 1, nie zwalnia jednak administratora danych z obowiązku przestrzegania pozostałych wymogów przewidzianych w RODO.

3. W art. 56 i 57 Traktatu o funkcjonowaniu Unii Europejskiej określono i uregulowano kwestię swobody świadczenia usług w Unii Europejskiej. Przyjęto szczególne środki prawodawcze UE w odniesieniu do „usług społeczeństwa informacyjnego"[3]. Usługi te obejmują „każdą usługę normalnie świadczoną za wynagrodzeniem, na odległość, drogą elektroniczną i na indywidualne żądanie odbiorcy usług". Definicja ta obejmuje usługi nieopłacane bezpośrednio przez osoby, które są ich odbiorcami[4], takie jak

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).
[2] Zobacz również motyw 44.
[3] Zobacz np. dyrektywę (UE) 2015/1535 Parlamentu Europejskiego i Rady oraz art. 8 RODO.
[4] Zobacz motyw 18 dyrektywy 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego.

usługi online finansowane za pomocą reklamy. „Usługi online" w rozumieniu niniejszych wytycznych odnoszą się do „usług społeczeństwa informacyjnego".

4. Rozwój prawa Unii odzwierciedla kluczowe znaczenie usług online w nowoczesnym społeczeństwie. Rozpowszechnianie się stale dostępnego mobilnego Internetu i powszechna dostępność urządzeń skomunikowanych umożliwiły rozwój usług online w dziedzinach, takich jak media społecznościowe, e-handel, wyszukiwanie w Internecie, komunikacja i podróże. Podczas gdy niektóre z tych usług są finansowane z płatności użytkownika, inne są świadczone bez płatności pieniężnych ze strony konsumenta, zamiast tego finansowane są ze sprzedaży usług reklamowych online umożliwiających dotarcie do osób, których dane dotyczą. Do celów takiej reklamy zachowanie użytkownika śledzi się często w sposób, którego użytkownik nie jest świadomy[5] i może nie wynikać bezpośrednio z charakteru świadczonej usługi, co w praktyce prawie uniemożliwia osobie, której dane dotyczą, dokonanie świadomego wyboru co do wykorzystania jej danych.

5. W tym kontekście Europejska Rada Ochrony Danych[6] (EROD) uważa za stosowne udzielenie wskazówek co do stosowania art. 6 ust. 1 lit. b) w odniesieniu do przetwarzania danych osobowych w kontekście usług online, aby zagwarantować powoływanie się na tę podstawę prawną jedynie w stosownych przypadkach.

6. Grupa Robocza Art. 29 wyraziła wcześniej stanowisko na temat podstawy odwołującej się do konieczności przetwarzania w celu wykonania umowy na podstawie dyrektywy 95/46/WE w swojej opinii w sprawie pojęcia uzasadnionych interesów administratora danych[7]. W ujęciu ogólnym wytyczne te pozostają istotne dla art. 6 ust. 1 lit. b) i RODO.

1.2 Zakres stosowania wytycznych

7. Niniejsze wytyczne dotyczą stosowania art. 6 ust. 1 lit. b) w odniesieniu do przetwarzania danych osobowych w kontekście umów o świadczenie usług online, niezależnie od sposobu finansowania tych usług. Niniejsze wytyczne określą elementy zgodnego z prawem przetwarzania na podstawie art. 6 ust. 1 lit. b) RODO i uwzględniają koncepcję „niezbędności" w zakresie, w jakim dotyczy ona przetwarzania „niezbędnego do wykonania umowy".

8. Przepisy dotyczące ochrony danych regulują ważne aspekty interakcji między usługami online a ich użytkownikami, obowiązują jednak również inne przepisy. Regulacja usług online wiąże się z wielofunkcyjnymi obowiązkami w takich dziedzinach jak, między innymi, prawo ochrony konsumentów i prawo konkurencji. Kwestie te wykraczają poza zakres niniejszych wytycznych.

9. Mimo że art. 6 ust. 1 lit. b) można stosować wyłącznie w kontekście umów, w niniejszych wytycznych nie zawarto ogólnej opinii na temat ważności umów o świadczenie usług online, ponieważ leży to poza zakresem kompetencji EROD. Umowy i postanowienia umowy muszą jednak być zgodne z wymogami prawa umów oraz, jak w przypadku umów konsumenckich, przepisami dotyczącymi ochrony konsumentów, aby przetwarzanie w oparciu o te postanowienia zostało uznane za rzetelne i zgodne z prawem.

10. Poniżej przedstawiono kilka ogólnych uwag na temat zasady ochrony danych, nie omówiono jednak wszystkich kwestii związanych z ochroną danych, które mogą pojawić się podczas przetwarzania na podstawie art. 6 ust. 1 lit. b). Administratorzy danych zawsze zapewniają zgodność z zasadami ochrony danych określonymi w art. 5 i wszystkimi pozostałymi wymogami RODO, oraz w stosownych przypadkach, przepisami dotyczącymi prywatności i łączności elektronicznej.

[5] W tym względzie administratorzy danych powinni wypełniać obowiązki w zakresie przejrzystości określone w RODO.
[6] Ustanowiona na podstawie art. 68 RODO.
[7] Grupa Robocza Art. 29, Opinia 06/2014 w sprawie pojęcia uzasadnionych interesów administratora danych zawartego w art. 7 dyrektywy 95/46/WE. Zobacz w szczególności s. 11, 16, 17, 18 i 55.

2 CZĘŚĆ 2 – ANALIZA ART. 6 UST. 1 LIT. B)

2.1 Uwagi ogólne

11. Podstawę prawną przetwarzania danych na podstawie art. 6 ust. 1 lit. b) należy rozpatrywać w kontekście RODO jako całości, celów o których mowa w art. 1 oraz obowiązku przetwarzania danych osobowych przez administratorów danych, zgodnie z zasadami ochrony danych na podstawie art. 5. Powyższe obejmuje przetwarzanie danych osobowych w sposób rzetelny i przejrzysty oraz zgodny z obowiązkami w zakresie ograniczenia celu i minimalizacji danych.

12. Zgodnie z art. 5 ust. 1 lit. a) RODO dane osobowe muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą. Zasada rzetelności obejmuje, między innymi, uwzględnienie rozsądnych oczekiwań[8] osób, których dane dotyczą, uwzględnienie ewentualnych negatywnych skutków przetwarzania dla takich osób oraz uwzględnienie relacji i potencjalnych skutków braku równowagi między osobami, których dane dotyczą, a administratorem danych.

13. Jak wskazano, umowy o świadczenie usług online, aby były zgodne z prawem, muszą być ważne na podstawie mającego zastosowanie prawa umów. Przykładem istotnego czynnika jest to, czy osoba, której dane dotyczą, jest dzieckiem. W takim przypadku (oprócz spełnienia wymogów RODO, w tym wymogów dotyczących „szczególnej ochrony" dzieci)[9], administrator danych musi zapewnić zgodność z odpowiednimi przepisami krajowymi dotyczącymi zdolności dzieci do zawierania umów. Ponadto aby zapewnić zgodność z zasadami rzetelności i zgodności z prawem administrator danych musi spełnić inne wymogi prawne. Na przykład w przypadku umów konsumenckich zastosowanie może mieć dyrektywa 93/13/EWG w sprawie nieuczciwych warunków w umowach konsumenckich[10]. Przepisy art. 6 ust. 1 lit. b) nie ograniczają się do umów podlegających prawu państwa członkowskiego EOG[11].

14. W art. 5 ust. 1 lit. b) RODO przewidziano zasadę ograniczenia celu, zgodnie z którą dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami.

15. W art. 5 ust. 1 lit. c) RODO przewidziano zasadę minimalizacji danych, tj. przetwarzania danych w zakresie ograniczonym do tego, co niezbędne do osiągnięcia celu. Ocena ta uzupełnia oceny niezbędności na podstawie art. 6 ust. 1 lit. b).

[8] Oczekuje się, że niektóre dane osobowe pozostaną prywatne lub będą przetwarzane w określony sposób, a osoba, której dane dotyczą, nie powinna być zaskoczona tym, że jej dane są przetwarzane. W RODO koncepcja „rozsądnych oczekiwań" została wyraźnie przywołana w motywach 47 i 50 w odniesieniu do art. 6 ust. 1 lit. f) i art. 6 ust. 4.
[9] Zobacz motyw 38, który przewiduje szczególną ochronę danych osobowych dzieci, gdyż mogą one być mniej świadome ryzyka, konsekwencji, zabezpieczeń i praw przysługujących im w związku z przetwarzaniem danych osobowych.
[10] Postanowienia umowy, które nie były indywidualnie negocjowane, mogą być uznane za nieuczciwe, zgodnie z dyrektywą w sprawie nieuczciwych warunków w umowach konsumenckich „jeśli stoją w sprzeczności z wymogami dobrej wiary, powodują znaczącą nierównowagę wynikających z umowy praw i obowiązków stron ze szkodą dla konsumenta". Podobnie jak w przypadku obowiązku przejrzystości, o którym mowa w RODO, dyrektywa w sprawie nieuczciwych warunków w umowach konsumenckich nakłada obowiązek stosowania prostego i zrozumiałego języka. Przetwarzanie danych osobowych na podstawie postanowienia, które zgodnie z dyrektywą w sprawie nieuczciwych warunków w umowach konsumenckich jest postanowieniem nieuczciwym, nie jest zgodne z wymogiem zawartym w art. 5 ust. 1 lit. a) RODO dotyczącym zgodności z prawem i rzetelności przetwarzania.
[11] Rozporządzenie w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych ma zastosowanie do niektórych administratorów danych spoza EOG; zob. art. 3 RODO.

16. Zarówno zasada ograniczenia celu jak i minimalizacji danych mają szczególne znaczenie w umowach o świadczenie usług online, które zazwyczaj nie podlegają indywidualnym negocjacjom. Postęp technologiczny umożliwia administratorom danych łatwe gromadzenie i przetwarzanie większej ilości danych osobowych niż kiedykolwiek wcześniej. W związku z tym istnieje poważne ryzyko, że administratorzy danych będą dążyć do zawierania w umowach warunków ogólnych przetwarzania w celu maksymalnego zwiększenia możliwości zbierania i wykorzystywania danych, bez stosownego określania tych celów i uwzględnienia obowiązków dotyczących minimalizacji danych. Grupa Robocza Art. 29 stwierdziła wcześniej:

> *„Cel zbierania danych musi być jasno i konkretnie określony: musi być wystarczająco szczegółowy, aby określić, jaki rodzaj przetwarzania danych jest objęty określonym celem, a jaki nie jest ,oraz aby umożliwić ocenę zgodności z prawem i zastosowanie zabezpieczeń ochrony danych. Z tych powodów cel, który jest niejednoznaczny lub ogólny, taki jak na przykład »poprawa doświadczeń użytkowników«, »cele marketingowe«, »cele bezpieczeństwa informatycznego« lub »przyszłe badania« – bez podania szczegółów – co do zasady nie będzie spełniał kryteriów »konkretności«.* [12]

2.2 Interakcja treści art. 6 ust. 1 lit. b) z pozostałymi podstawami prawnymi przetwarzania

17. W przypadku gdy przetwarzanie danych nie jest uważane za „niezbędne do wykonania umowy", tj. gdy usługę, której dotyczy wniosek, można świadczyć bez konkretnego przetwarzania danych, EROD uznaje możliwość stosowania innej podstawy prawnej, o ile spełnione są odpowiednie warunki. W szczególności w pewnych okolicznościach właściwsze może być powoływanie się na dobrowolną zgodę na podstawie art. 6 ust. 1 lit. a). W innych przypadkach bardziej odpowiednią podstawę prawną przetwarzania może stanowić art. 6 ust. 1 lit. f). Podstawę prawną należy określić na początku przetwarzania, przy czym należy wskazać ją w informacjach podawanych osobom, których dane dotyczą zgodnie z art. 13 i 14.

18. Istnieje możliwość, że celowi i kontekstowi danej operacji przetwarzania lepiej odpowiadać będzie podstawa prawna inna niż określona w art. 6 ust. 1 lit. b). Wskazanie odpowiedniej podstawy prawnej wiąże się z zasadami rzetelności i ograniczenia celu[13].

19. W wytycznych Grupy Roboczej Art. 29 dotyczących zgody wskazano wyraźnie, że „jeżeli administrator zamierza przetwarzać dane osobowe, które są faktycznie niezbędne do wykonania umowy, zgoda nie jest właściwą, zgodną z prawem podstawą". Europejska Rada Ochrony Danych uważa natomiast, że w przypadku gdy przetwarzanie nie jest faktycznie niezbędne do wykonania umowy, może ono mieć miejsce tylko wtedy, gdy opiera się na innej odpowiedniej podstawie prawnej[14].

20. Administratorzy danych, zgodnie ze swoimi zobowiązaniami w zakresie przejrzystości, powinni dopilnować, aby nie pojawiły się nieporozumienia w kwestii mającej zastosowanie podstawy prawnej. Jest to szczególnie istotne w przypadku, gdy właściwą podstawą prawną jest art. 6 ust. 1 lit. b), a umowę o świadczenie usług online zawierają osoby, których dane dotyczą. W zależności od okoliczności, osoby, których dane dotyczą, mogą odnieść błędne wrażenie, że podpisując umowę lub akceptując warunki świadczenia usług wyrażają zgodę zgodnie z art. 6 ust. 1 lit. a). Jednocześnie administrator danych może błędnie zakładać, że podpisanie umowy stanowi zgodę w rozumieniu art. 6 ust. 1 lit. a). Są to zupełnie inne pojęcia. Należy odróżnić zaakceptowanie warunków świadczenia usługi w celu zawarcia umowy od wyrażenia zgody w rozumieniu art. 6 ust. 1 lit. a), ponieważ pojęcia te mają różne wymogi i konsekwencje prawne.

21. W odniesieniu do przetwarzania szczególnych kategorii danych osobowych Grupa Robocza Art. 29, w swoich wytycznych dotyczących zgody, zauważa, że:

> *„W art. 9 ust. 2 nie przewidziano, by charakter danych »niezbędnych do wykonania umowy« był wyjątkiem od ogólnego zakazu przetwarzania szczególnych kategorii danych. W związku z tym administratorzy i państwa członkowskie, które znajdują się w takiej sytuacji, powinni zbadać konkretne wyjątki przewidziane w art. 9 ust. 2 lit. b)–j). Jeżeli żaden z wyjątków przewidzianych w przepisach lit. b)–j) nie będzie miał zastosowania, jedynym możliwym wyjątkiem, który można zastosować zgodnie z prawem do przetwarzania takich danych, jest uzyskanie wyraźniej zgody zgodnie z przewidzianymi w RODO warunkami uzyskania ważnej zgody"*[15].

2.3 Zakres zastosowania art. 6 ust. 1 lit. b)

22. Artykuł 6 ust. 1 lit. b) stosuje się w przypadku spełnienia jednego z dwóch warunków: przetwarzanie jest obiektywnie niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub przetwarzanie jest obiektywnie niezbędne do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy.

2.4 Niezbędność

23. Niezbędność przetwarzania jest warunkiem wstępnym dla obu części art. 6 ust. 1 lit. b). Należy przede wszystkim zauważyć, że pojęcie tego, co jest "niezbędne do wykonania umowy" nie jest jedynie oceną tego, na co zezwalają postanowienia umowy lub co obejmuje jej zakres. Pojęcie niezbędności ma odrębne znaczenie w prawie Unii Europejskiej, które musi odzwierciedlać cele prawa o ochronie danych[16]. W związku z tym obejmuje ono również podstawowe prawo do ochrony prawnej życia prywatnego i ochrony danych osobowych[17], jak również wymogi zasad ochrony danych, w tym w szczególności zasady rzetelności.

24. Punktem wyjścia jest określenie celu przetwarzania oraz, a kontekście stosunku umownego mogą istnieć różne cele przetwarzania. Cele te należy jasno określić i powiadomić o nich osobę, której dane dotyczą, zgodnie z obowiązkami administratora danych w zakresie ograniczenia celu i przejrzystości.

25. Ocena tego, co jest „niezbędne" obejmuje połączoną, opartą na faktach ocenę przetwarzania „w odniesieniu do zamierzonego celu oraz tego, czy przetwarzanie jest mniej inwazyjne w porównaniu z

[12] Grupa Robocza Art. 29, Opinia 03/2013 w sprawie ograniczenia celu (WP203), s. 15–16.
[13] Określenie przez administratorów danych odpowiedniej podstawy prawnej zgodnie z zasadą rzetelności będzie trudne bez wyraźnego wskazania w pierwszej kolejności celów przetwarzania lub jeżeli zakres przetwarzania danych wykracza poza zakres niezbędny do osiągnięcia określonych celów.
[14] Więcej informacji na temat skutków związanych z art. 9 można znaleźć w wytycznych Grupy Roboczej Art. 29 dotyczących zgody na mocy rozporządzenia 2016/679 (WP259), zatwierdzonych przez EROD, s. 19–20.

[15] Grupa Robocza Art. 29, Wytyczne dotyczące zgody na mocy rozporządzenia 2016/679 (WP259), zatwierdzone przez EROD, s. 19.
[16] Trybunał Sprawiedliwości Unii Europejskiej w sprawie Heinz Huber przeciwko Bundesrepublik Deutschland stwierdził, że „mamy tutaj zatem do czynienia z autonomicznym pojęciem prawa wspólnotowego [konieczności], którego wykładnia winna w pełni odpowiadać celowi tej dyrektywy [dyrektywy 95/46] sformułowanemu w jej art. 1 ust. 1". Wyrok TSUE w sprawie C 524/06, Heinz Huber przeciwko Bundesrepublik Deutschland, 18 grudnia 2008 r. punkt 52.
[17] Zobacz art. 7 i 8 Karty praw podstawowych Unii Europejskiej

innymi metodami osiągnięcia tego samego celu"[18]. Jeżeli istnieją realne, mniej inwazyjne opcje, przetwarzanie nie jest „niezbędne"[19]. Artykuł 6 ust. 1 lit. b) nie obejmuje przetwarzania, które jest przydatne, ale nie jest obiektywnie niezbędne do wykonania usługi objętej umową lub podjęcia odpowiednich działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy, nawet jeżeli jest ono niezbędne do innych celów biznesowych administratora danych.

2.5 Niezbędne do wykonania umowy zawartej z osobą, której dane dotyczą

26. Administrator danych może powołać się na pierwszą opcją na podstawie art. 6 ust. 1 lit. b) w celu przetwarzania danych osobowych, jeżeli – zgodnie ze swoimi obowiązkami w zakresie odpowiedzialności wynikającymi z art. 5 ust. 2 – może wykazać, że przetwarzanie odbywa się w kontekście ważnej umowy zawartej z osobą, której dane dotyczą, oraz że przetwarzanie jest niezbędne do wykonania tej *konkretnej umowy* zawartej z osobą, której dane dotyczą. Jeżeli administratorzy danych nie mogą wykazać, że: a) umowa istnieje, b) umowa jest ważna na mocy obowiązujących przepisów prawa umów, oraz c) przetwarzanie jest obiektywnie niezbędne w celu wykonania umowy, administrator danych powinien rozważyć zastosowanie innej podstawy prawnej przetwarzania.

27. Samo odniesienie do przetwarzania danych lub wspomnienie o przetwarzaniu danych w umowie nie jest wystarczające, aby takie przetwarzanie objąć zakresem stosowania art. 6 ust. 1 lit. b). Z drugiej strony przetwarzanie może być obiektywnie niezbędne, nawet jeśli nie określono tego wyraźnie w umowie. W każdym przypadku administrator danych musi spełnić swoje obowiązki w zakresie przejrzystości. Jeżeli administrator danych chce ustalić, że podstawą przetwarzania danych jest wykonanie umowy zawartej z osobą, której dane dotyczą, ważne jest dokonanie oceny, co jest *obiektywnie niezbędne* do jej wykonania. „Niezbędne do wykonania" wyraźnie świadczy o tym, że wymaga się czegoś więcej niż tylko klauzuli umownej. Jest to również oczywiste w świetle art. 7 ust. 4. Chociaż przepis ten dotyczy jedynie ważności zgody, w sposób obrazowy wprowadza rozróżnienie pomiędzy czynnościami przetwarzania danych niezbędnymi do wykonania umowy a *klauzulami* uzależniającymi świadczenie usługi od dokonania pewnych czynności przetwarzania, które w rzeczywistości nie są niezbędne do wykonania umowy.

28. W tym względzie EROD popiera wytyczne przyjęte wcześniej przez Grupę Roboczą Art. 29 w sprawie równoważnego przepisu na mocy poprzedniej dyrektywy, że „przetwarzanie danych jest konieczne dla realizacji umowy, której stroną jest osoba, której dane dotyczą":

> *„[...] trzeba interpretować w sposób zawężający. Nie obejmuje on sytuacji, w których przetwarzanie nie jest rzeczywiście konieczne dla realizacji umowy, ale raczej jednostronnie narzucone osobie, której dane dotyczą, przez administratora danych. Również fakt, że niektóre czynności przetwarzania danych są objęte umową, nie oznacza automatycznie, że przetwarzanie to jest niezbędne do jej realizacji.* [...] *Nawet jeśli ta działalność związana z przetwarzaniem jest wyraźnie wymieniona drobnym drukiem w umowie, sam ten fakt nie czyni jej »niezbędną« dla realizacji umowy"*[20].

29. Europejska Rada Ochrony Danych odwołuje się również do tych samych wytycznych Grupy Roboczej Art. 29 stwierdzając, że:

> *„Istnieje tu wyraźny związek pomiędzy oceną konieczności a zgodnością z zasadą celowości. Istotne jest określenie dokładnego powodu umowy, czyli jej istoty i podstawowego celu, ponieważ to względem nich będzie badane, czy przetwarzanie danych jest konieczne dla realizacji tej umowy"*[21].

30. Oceniając, czy art. 6 ust. 1 lit. b) stanowi właściwą podstawę prawną przetwarzania danych w kontekście usług online objętych umową, należy uwzględnić szczególne zamierzenie, cel lub przeznaczenie tej usługi. Do celów stosowalności art. 6 ust. 1 lit. b) wymaga się, aby przetwarzanie danych było *obiektywnie niezbędne* do osiągnięcia celu, jakim jest świadczenie tej usługi na rzecz osoby, której dane dotyczą. Nie wyłącza się przetwarzania danych dotyczących płatności w celu pobrania opłaty za usługę. Administrator danych powinien być w stanie wykazać, w jaki sposób główny przedmiot *konkretnej umowy* zawartej z *osobą, której dane dotyczą*, nie będzie mógł zostać faktycznie realizowany bez *przetwarzania danych osobowych*. Istotną kwestią jest tu związek między danymi osobowymi i operacjami przetwarzania a wykonaniem lub niewykonaniem usługi świadczonej na podstawie umowy.

31. Umowy na usługi cyfrowe mogą zawierać wyraźne postanowienia nakładające dodatkowe warunki w zakresie między innymi reklamy, płatności czy plików cookie. W umowie nie można w sposób sztuczny rozszerzać kategorii danych osobowych ani rodzajów operacji przetwarzania, które administrator danych musi wykonać w celu wykonania umowy w rozumieniu art. 6 ust. 1 lit. b).

32. Administrator danych powinien być w stanie uzasadnić niezbędność przetwarzania poprzez zawarcie odniesienia do podstawowego i wspólnie uzgodnionego celu umowy. Zależy to nie tylko od interesów administratora danych, ale również od uzasadnionych interesów osoby, której dane dotyczą, w momencie zawierania umowy oraz od tego, czy umowę można nadal uznać za „wykonaną" bez przetwarzania takich danych. Administrator danych może uznać, że przetwarzanie jest niezbędne do celów umowy, ważne jest jednak, aby uważnie przeanalizował interes przeciętnej osoby, której dane dotyczą, w celu zapewnienia rzeczywistego wzajemnego zrozumienia celu umowy.

33. To, czy art. 6 ust. 1 lit. b) ma zastosowanie, można ocenić odpowiadając na poniższe pytania:

- Jaki jest charakter usługi świadczonej na rzecz osoby, które dane dotyczą? Jakie są jej cechy charakterystyczne?
- Jakie jest dokładne uzasadnienie zawarcia umowy (tj. jej istota i główny przedmiot?
- Jakie są istotne elementy umowy?
- Jakie są wzajemne interesy i oczekiwania stron umowy? W jaki sposób usługa jest upowszechniana lub reklamowana osobie, której dane dotyczą? Czy zwykły użytkownik

[18] Zobacz Instrumentarium Europejskiego Inspektora Ochrony Danych: Ocena konieczności środków ograniczających podstawowe prawo do ochrony danych osobowych, s. 5.

[19] W sprawie *Volker und Markus Schecke GbR i Hartmut Eifert przeciwko Land Hessen*, TSUE orzekł, że badając konieczność przetwarzania danych osobowych, organ ustawodawczy musi uwzględnić alternatywne, mniej inwazyjne środki. Wyrok TSUE w sprawach połączonych C92/09 i C93/09, Volker und Markus Schecke GbR oraz Hartmut Eifert przeciwko Land Hessen, z dnia 9 listopada 2010 r. Trybunał powtórzył to samo w wyroku w sprawie Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde przeciwko Rīgas pašvaldības SIA „Rīgas satiksme", w którym orzekł, że: „Jeśli chodzi o przesłankę dotyczącą konieczności przetwarzania danych, należy przypomnieć, że odstępstwa od zasady ochrony danych osobowych i jej ograniczenia powinny być stosowane jedynie wtedy, gdy jest to absolutnie konieczne". Wyrok TSUE w sprawie C-13/16 *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde przeciwko Rīgas pašvaldības SIA „Rīgas satiksme"*, punkt 30. Wszelkie ograniczenia korzystania z prawa do ochrony prawnej życia prywatnego i ochrony danych osobowych w odniesieniu do przetwarzania danych osobowych wymagają przeprowadzenia ścisłej oceny konieczności, zob. Instrumentarium EIOD: Ocena konieczności środków ograniczających podstawowe prawo do ochrony danych osobowych, s. 7.

[20] Grupa Robocza Art. 29, Opinia 06/2014 w sprawie pojęcia uzasadnionych interesów administratora danych zawartego w art. 7 dyrektywy 95/46/WE (WP217) s.16–17.

[21] Ibidem, s. 17.

usługi może zasadnie oczekiwać, że z uwagi na charakter usługi planowane przetwarzanie będzie miało miejsce w celu wykonania umowy, której jest stroną?

34. Jeżeli ocena tego co jest „niezbędne do wykonania umowy", którą należy przeprowadzić przed rozpoczęciem przetwarzania danych wykaże, że zamierzone przetwarzanie danych wykracza poza zakres tego, co jest obiektywnie niezbędne o wykonania umowy, nie oznacza to, że takie przyszłe przetwarzanie danych jest samo w sobie niezgodne z prawem. Jak przedstawiono powyżej, w art. 6 wyraźnie wskazuje się, że administrator danych może potencjalnie skorzystać z innej podstawy prawnej przed rozpoczęciem przetwarzania[22].

35. Jeżeli w trakcie trwania usługi wprowadza się nową technologię zmieniającą sposób przetwarzania danych osobowych lub usługa zmieni się w inny sposób, powyższe kryteria należy poddać ponownej ocenie, aby określić czy na podstawie art. 6 ust. 1 lit. b) można dokonać jakichkolwiek nowych lub zmienionych operacji przetwarzania.

Przykład 1

Osoba, której dane dotyczą, kupuje produkty od internetowego sprzedawcy detalicznego. Osoba, której dane dotyczą, chce zapłacić kartą kredytową oraz aby produkty dostarczono na jej adres zamieszkania. Aby wykonać umowę sprzedawca detaliczny musi przetworzyć informacje dotyczące karty kredytowej i adres do celów rozliczeniowych osoby, której dane dotyczą, w celu dokonania płatności oraz adres zamieszkania osoby, której dane dotyczą, w celu dokonania dostawy. Artykuł 6 ust. 1 lit. b) ma zatem zastosowanie jako podstawa prawna dla tych działań związanych z przetwarzaniem.

Jeżeli jednak klient wybrał opcję wysyłki do punktu odbioru, przetwarzanie adresu zamieszkania osoby, której dane dotyczą, nie jest już niezbędne do wykonania umowy kupna-sprzedaży. Przetwarzanie adresu osoby, której dane dotyczą, w tym kontekście będzie wymagało innej podstawy prawnej niż ta opisana w art. 6 ust. 1 lit. b).

Przykład 2

Ten sam internetowy sprzedawca detaliczny chce zbudować profile użytkowników w zakresie ich gustów i wyborów stylów życia na podstawie ich wizyt na stronie internetowej. Wykonanie umowy kupna-sprzedaży nie zależy od stworzenia takich profili. Nawet jeśli profilowanie jest wyraźnie wymienione w umowie, sam ten fakt nie czyni go „niezbędnym" dla wykonania umowy. Jeżeli internetowy sprzedawca detaliczny chce dokonać takiego profilowania, musi oprzeć się na innej podstawie prawnej.

36. W granicach prawa umów oraz, w stosownych przypadkach, prawa ochrony konsumentów, administratorzy danych mają swobodę projektowania swojej działalności, usług i umów. W niektórych przypadkach administrator danych może zechcieć połączyć kilka odrębnych usług lub elementów usługi o różnych podstawowych celach, cechach lub przesłankach w ramach jednej umowy. Takie

[22] Zobacz Grupa Robocza Art. 29, Wytyczne dotyczące zgody na mocy rozporządzenia 2016/679 (WP259), zatwierdzone przez EROD, s. 31, zgodnie z którymi: „W RODO nie przewidziano możliwości zastąpienia jednej zgodnej z prawem podstawą inną podstawą".

podejście może prowadzić do konieczności zaakceptowania całości umowy bądź jej odrzucenia przez osoby, których dane dotyczą, a które mogą być tylko zainteresowane jedną z tych usług.

37. W zakresie prawa ochrony danych osobowych administratorzy danych biorą pod uwagę, że przewidziana działalność związana z przetwarzaniem musi mieć odpowiednią podstawę prawną. W przypadku gdy umowa obejmuje kilka odrębnych usług lub elementów usługi, które w rzeczywistości można wykonywać niezależnie od siebie, powstaje pytanie, w jakim zakresie art. 6 ust. 1 lit. b) może służyć jako podstawa prawna. Zastosowanie art. 6 ust. 1 lit. b) należy ocenić *oddzielnie* w kontekście każdej z tych usług, uwzględniając to, co jest obiektywnie niezbędne do wykonania każdej z poszczególnych usług, których aktywnie zażądała osoba, której dane dotyczą, lub dokonała rejestracji, by z nich korzystać. W wyniku oceny może okazać się, że pewne działania związane z przetwarzaniem nie są niezbędne do wykonania poszczególnych usług, których zażądała osoba, której dane dotyczą, a raczej niezbędne w odniesieniu do szerszego modelu biznesowego administratora danych. W takim przypadku art. 6 ust. 1 lit. b) nie będzie podstawą prawną dla tych działań. Podstawą dla takiego przetwarzania mogą być jednak inne podstawy prawne, jak np. art. 6 ust. 1 lit. a) lub f), pod warunkiem, że spełnione są odpowiednie kryteria. W związku z tym ocena możliwości zastosowania art. 6 ust. 1 lit. b) nie ma wpływu na zgodność z prawem umowy lub łączenia usług jako takich.

38. Grupa Robocza Art. 29 stwierdziła wcześniej, że postawę prawną stosuje się tylko do tego, co jest konieczne dla realizacji umowy[23]. Z związku z tym, nie ma ona zastosowania do wszystkich dalszych działań wywołanych niezgodnością ani do innych incydentów zaistniałych podczas wykonywania umowy. Pewne działania mogą być jednak w sposób rozsądny przewidziane i niezbędne w ramach zwykłego stosunku umownego, takie jak wysyłanie formalnych wezwań do zapłaty lub usunięcia błędów lub opóźnień w wykonaniu umowy. Artykuł 6 ust. 1 lit. b) może być podstawą do przetwarzania danych osobowych niezbędnego w związku z takimi działaniami.

Przykład 3

Przedsiębiorstwo sprzedaje produkty online. Klient kontaktuje się z przedsiębiorstwem, ponieważ kolor zakupionego produktu różni się od tego, co uzgodniono. Artykuł 6 ust. 1 lit. b) może być podstawą przetwarzania danych osobowych klienta w celu zlikwidowania tego problemu.

39. Gwarancja umowna może stanowić część realizacji umowy, a tym samym przechowywanie pewnych danych przez określony czas po zakończeniu wymiany towarów/usług/płatności do celów gwarancji może być niezbędne do wykonania umowy.

2.6 Rozwiązanie umowy

40. Administrator danych musi wskazać odpowiednią podstawę prawną dla planowanych operacji przetwarzania przed jego rozpoczęciem. Jeżeli art. 6 ust. 1 lit. b) stanowi podstawę dla niektórych lub wszystkich czynności przetwarzania administrator danych powinien przewidzieć co się stanie jeżeli umowa zostanie rozwiązana[24].

[23] Grupa Robocza Art. 29 (2014), Opinia 06/2014 w sprawie pojęcia uzasadnionych interesów administratora danych zawartego w art. 7 dyrektywy 95/46/WE (WP217) s.17–18.

[24] Jeśli umowa zostanie następnie unieważniona, takie unieważnienie będzie miało wpływ na zgodność z prawem (w rozumieniu art. 5 ust. 1 lit. a)) dalszych czynności przetwarzania. Nie oznacza to jednak, że wybór art. 6 ust. 1 lit. b) jako podstawy prawnej jest błędny.

41. W przypadku gdy przetwarzanie danych osobowych opiera się na art. 6 ust. 1 lit. b) a umowa zostanie rozwiązana w całości, co do zasady, przetwarzanie tych danych nie będzie już niezbędne do wykonania umowy i w związku z tym administrator danych będzie musiał zaprzestać przetwarzania. Osoba, której dane dotyczą, mogła podać swoje dane osobowe w kontekście stosunku umownego, myśląc że dane będą przetwarzane jedynie jako niezbędny element tego stosunku. W związku z tym zamiana pierwotnej podstawy prawnej na nową podstawę prawną w momencie, gdy ta pierwsza przestaje istnieć, jest z reguły działaniem nieuczciwym.

42. Rozwiązanie umowy może pociągać za sobą pewne obciążenia administracyjne, takie jak zwrot towarów lub płatności. Związane z tym przetwarzanie może opierać się na art. 6 ust. 1 lit. b).

43. Zgodnie z art. 17 ust. 1 lit. a) dane osobowe są usuwane, gdy nie są już niezbędne do celów, w których zostały zebrane. Nie ma to jednak zastosowania, jeżeli przetwarzanie danych jest niezbędne do pewnych określonych celów, w tym do wywiązania się z obowiązku prawnego na podstawie art. 17 ust. 3 lit. b) lub do ustalenia, dochodzenia lub obrony roszczeń zgodnie z art. 17 ust. 3 lit. e). W praktyce, jeżeli administratorzy widzą ogólną potrzebę prowadzenia rejestrów do celów prawnych, powinni wskazać podstawę prawną na początku przetwarzania i od początku wyraźnie określić, przez jaki okres planują przechowywać rejestry do tych celów prawnych po rozwiązaniu umowy. W takim przypadku nie muszą usuwać danych po rozwiązaniu umowy.

44. W każdym przypadku może się zdarzyć, że na początku przetwarzania określono kilka operacji przetwarzania danych o odrębnych celach i podstawach prawnych. Dopóki te operacje przetwarzania pozostają zgodne z prawem, a administrator danych poinformował o tych operacjach w momencie rozpoczęcia przetwarzania zgodnie z obowiązkami w zakresie przejrzystości określonymi w RODO, przetwarzanie danych osobowych dotyczących osoby, której dane dotyczą, do tych odrębnych celów będzie nadal możliwe po rozwiązaniu umowy.

Przykład 4

Dostawca usługi online oferuje usługę subskrypcji, którą można w dowolnym momencie odwołać. Po zawarciu umowy o świadczenie usługi administrator danych przekazuje osobie, której dane dotyczą, informacje o przetwarzaniu danych osobowych.

Administrator danych wyjaśnia, między innymi, że dopóki obowiązuje umowa, będzie przetwarzać dane dotyczące korzystania z usługi do celów wystawiania faktur. Właściwą podstawą prawną jest art. 6 ust. 1 lit. b), ponieważ przetwarzanie do celów fakturowania uznaje się za obiektywnie niezbędne do wykonania umowy. Jeżeli jednak umowa zostanie rozwiązana i przy założeniu, że nie istnieją żadne istotne roszczenia ani wymogi prawne uzasadniające zatrzymanie danych, historia użytkowania jest usuwana.

Ponadto administrator danych informuje osoby, których dane dotyczą, że na mocy prawa krajowego ma zobowiązanie prawne do zatrzymania pewnych danych osobowych do celów rachunkowości przez określoną liczbę lat. Właściwą podstawą prawną jest art. 6 ust. 1 lit. c), a dane są przechowywane nawet w przypadku rozwiązania umowy.

2.7 Niezbędne do podjęcia działań przed zawarciem umowy

45. Drugą opcję przewidzianą w art. 6 ust. 1 lit. b) stosuje się w sytuacji, gdy *przetwarzanie jest niezbędne do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy*. Przepis ten odzwierciedla fakt, że wstępne przetwarzanie danych osobowych może być niezbędne przed zawarciem umowy w celu ułatwienia faktycznego jej zawarcia.

46. W momencie przetwarzania danych nie jest jasne, czy umowa zostanie faktycznie zawarta. Druga opcja przewidziana w art. 6 ust. 1 lit. b) może jednak mieć zastosowanie, o ile osoba, której dane dotyczą, wystąpi z żądaniem w kontekście ewentualnego zawarcia umowy, a przetwarzanie danych jest niezbędne do podjęcia wymaganych działań. Zgodnie z powyższym, jeżeli osoba, której dane dotyczą, kontaktuje się z administratorem danych w celu uzyskania informacji na temat oferty usług administratora danych, przetwarzanie danych osobowych osoby, której dane dotyczą, w celu udzielenia odpowiedzi na zapytanie można oprzeć na art. 6 ust. 1 lit. b).

47. W żadnym przypadku przepis ten nie obejmuje niezamówionego marketingu ani innego rodzaju przetwarzania dokonywanego wyłącznie z inicjatywy administratora danych lub na żądanie osoby trzeciej.

Przykład 5

Osoba, której dane dotyczą, podaje swój kod pocztowy, aby sprawdzić, czy dany dostawca usług działa na interesującym ją obszarze. Taki przypadek można uznać za przetwarzanie niezbędne do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy na podstawie art. 6 ust. 1 lit. b).

Przykład 6

W niektórych przypadkach instytucje finansowe mają obowiązek identyfikacji swoich klientów zgodnie z prawem krajowym. W związku z tym, przed zawarciem umowy z osobami, których dane dotyczą, bank zwraca się z prośbą o wgląd w ich dokumenty tożsamości.

W takim przypadku identyfikacja jest niezbędna do spełnienia przez bank jego zobowiązania prawnego, a nie do podjęcia działań na żądanie osoby, której dane dotyczą. W związku z tym właściwą podstawą nie jest art. 6 ust. 1 lit. b), lecz art. 6 ust. 1 lit. c).

3 CZĘŚĆ 3 – STOSOWANIE ART. 6 UST. 1 LIT. B) W OKREŚLONYCH SYTUACJACH

3.1 Przetwarzanie w celu „poprawy jakości usługi”[25]

48. Dostawcy usług online często gromadzą szczegółowe informacje na temat sposobu wykorzystywania usług przez użytkowników. W większości przypadków zbierania danych organizacyjnych związanych z usługą lub szczegółów dotyczących zaangażowania użytkownika nie można uznać za niezbędne do świadczenia usługi, ponieważ usługa może być świadczona bez przetwarzania takich danych osobowych. Usługodawca może jednak może opierać się na innych zgodnych z prawem podstawach przetwarzania danych, takich jak uzasadniony interes lub zgoda.

[25] Świadczenie usług online może również wymagać uwzględnienia dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/770 z dnia 20 maja 2019 r. w sprawie niektórych aspektów umów o dostarczanie treści cyfrowych i usług cyfrowych (Dz.U. L 136 z 22.05.2019, s. 1), która wejdzie w życie 1 stycznia 2022 r.

49. Europejska Rada Ochrony Danych uważa, że art. 6 ust. 1 lit. b) zasadniczo nie stanowi odpowiedniej i zgodnej z prawem podstawy przetwarzania do celów poprawy jakości usługi lub opracowania nowych funkcji w ramach istniejącej usługi. W większości przypadków użytkownik zawiera umowę na korzystanie z istniejącej usługi. O ile postanowienia umowy mogą rutynowo uwzględniać wprowadzanie ulepszeń i modyfikacji do usługi, takiego przetwarzania nie można uznać za obiektywnie niezbędne do wykonania umowy zawartej z użytkownikiem.

3.2 Przetwarzanie w celu „zapobiegania oszustwom"

50. Zgodnie z tym, co stwierdziła wcześniej Grupa Robocza Art. 29[26] przetwarzanie w celu zapobiegania oszustwom może obejmować między innymi monitorowanie i profilowanie klientów. Zdaniem EROD takie przetwarzanie może wykraczać poza zakres tego, co jest obiektywnie niezbędne do wykonania umowy zawartej z osobą, której dane dotyczą. Przetwarzanie danych osobowych bezwzględnie niezbędne do zapobiegania oszustwom może jednak stanowić prawnie uzasadniony interes administratora danych[27], a w związku z tym można je uznać za zgodne z prawem, o ile administrator danych spełni szczególne wymogi art. 6 ust. 1 lit. f) (prawnie uzasadniony interes). Podstawą takiego przetwarzania danych może być również art. 6 ust. 1 lit. c) (obowiązek prawny).

3.3 Przetwarzanie na potrzeby internetowej reklamy behawioralnej

51. Internetowa reklama behawioralna oraz związane z nią śledzenie i profilowanie osób, których dane dotyczą, są często stosowane do finansowania usług online. Grupa Robocza Art. 29 wyraziła wcześniej swoją opinię na temat takiego rodzaju przetwarzania stwierdzając, że:

> *„[konieczność przetwarzania w celu wykonania umowy] nie jest odpowiednią podstawą prawną w odniesieniu do tworzenia profilu dotyczącego upodobań i stylu życia użytkownika w oparciu o jego kliknięcia na stronie internetowej i zakupione przedmioty. Wynika to z tego, że administratorowi danych nie zlecono tworzenia profili, a raczej na przykład dostarczanie określonych towarów i usług".*[28]

52. Zasadniczo przetwarzanie danych osobowych do celów reklamy behawioralnej nie jest niezbędne do wykonania umowy na usługi online. Stwierdzenie, że umowa nie została wykonana ze względu na brak reklamy behawioralnej nie jest argumentem przekonującym. Jest to tym bardziej uzasadnione faktem, że osoby, których dane dotyczą, mają bezwzględne prawo wniesienia sprzeciwu wobec przetwarzania danych do celów marketingu bezpośredniego na podstawie art. 21.

53. Ponadto art. 6 ust. 1 lit. b) nie może stanowić podstawy prawnej dla internetowej reklamy behawioralnej tylko dlatego, że reklama taka pośrednio finansuje świadczenie usługi. Chociaż taki rodzaj przetwarzania może stanowić wsparcie dla świadczenia usługi, fakt ten sam w sobie nie wystarcza, aby wykazać, że jest ono niezbędne do wykonania danej umowy. Administrator danych musiałby wziąć pod uwagę czynniki przedstawione w ust. 33.

[26] Grupa Robocza Art. 29 (2014), Opinia 06/2014 w sprawie pojęcia uzasadnionych interesów administratora danych zawartego w art. 7 dyrektywy 95/46/WE (WP217), s. 17.
[27] Zobacz motyw 47, zdanie szóste.
[28] Grupa Robocza Art. 29 (2014), Opinia 06/2014 w sprawie pojęcia uzasadnionych interesów administratora danych zawartego w art. 7 dyrektywy 95/46/WE (WP217), s. 17.

54. Biorąc pod uwagę, że ochrona danych jest prawem podstawowym zagwarantowanym w art. 8 Karty praw podstawowych oraz że jednym z głównych celów RODO jest zapewnienie osobom, których dane dotyczą, kontroli nad dotyczącymi ich informacjami, danych osobowych nie można uznać za towar handlowy. Nawet jeżeli osoba, której dane dotyczą, może wyrazić zgodę na przetwarzanie danych osobowych[29], nie może na podstawie takiej zgody oddać przysługujących jej praw podstawowych[30].

55. Europejska Rada Ochrony Danych zauważa również, że zgodnie z wymogami dotyczącymi prywatności i łączności elektronicznej oraz istniejącą opinią Grupy Roboczej Art. 29 w sprawie reklamy behawioralnej[31] oraz dokumentem roboczym 02/2013 zawierającym wskazówki na temat uzyskiwania zgody na zapisywanie plików cookie[32], administratorzy danych muszą uzyskać uprzednią zgodę osób, których dane dotyczą, na umieszczenie plików cookie, które są niezbędne do udziału w reklamie behawioralnej.

56. Europejska Rada Ochrony Danych zauważa również, że śledzenia i profilowania użytkowników można dokonywać w celu identyfikacji grup osób o podobnych cechach, aby umożliwić kierowanie reklam do podobnych odbiorców. Takiego rodzaju przetwarzania nie można dokonywać na podstawie art. 6 ust. 1 lit. b), ponieważ nie można uznać, że śledzenie i porównywanie cech i zachowania użytkowników w celach związanych z reklamą kierowaną do innych osób jest obiektywnie niezbędne do wykonania umowy zawartej z użytkownikiem[33].

3.4 Przetwarzanie w celu personalizacji treści[34]

57. Europejska Rada Ochrony Danych przyjmuje do wiadomości, że personalizacja treści może (ale nie zawsze musi) stanowić nieodłączny i oczekiwany element niektórych usług online, a zatem w niektórych przypadkach można ją uznać za niezbędną do wykonania umowy zawartej z użytkownikiem usługi. To, czy taki rodzaj przetwarzania można postrzegać jako nieodłączny element usługi online, zależeć będzie od charakteru świadczonej usługi, oczekiwań przeciętnej osoby, której dane dotyczą, w świetle nie tylko warunków świadczenia usługi, ale również sposobu jej reklamowania użytkownikom, jak również od tego, czy usługę można świadczyć bez personalizacji. Jeżeli personalizacja treści nie jest obiektywnie niezbędna do wykonania danej umowy, na przykład gdy spersonalizowane treści służą zwiększeniu zaangażowania użytkownika w usługę, a nie stanowią jej integralnej części, administratorzy danych powinni, w stosownych przypadkach, rozważyć zastosowanie innej podstawy prawnej.

[29] Zobacz dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/770 z dnia 20 maja 2019 r. w sprawie niektórych aspektów umów o dostarczanie treści cyfrowych i usług cyfrowych.
[30] Oprócz samego faktu, że wykorzystywanie danych osobowych podlega regulacjom RODO, istnieją dodatkowe powody, dla których przetwarzanie danych osobowych różni się pojęciowo od płatności pieniężnych. Na przykład pieniądze są policzalne, co oznacza, że ceny można porównać na konkurencyjnym rynku, a płatności pieniężnych dokonuje się zazwyczaj przy udziale osoby, której dane dotyczą. Ponadto dane osobowe można wykorzystywać w ramach kilka usług jednocześnie. Jeżeli utraci się kontrolę nad danymi osobowymi, niekoniecznie uda się ją odzyskać.
[31] Grupa Robocza Art. 29, Opinia 2/2010 w sprawie internetowej reklamy behawioralnej (WP171).
[32] Grupa Robocza Art. 29, Dokument roboczy 2/2013 przedstawiający wytyczne w sprawie pozyskiwania zgody na zapisywanie plików cookie (WP208).
[33] Zobacz również Grupa Robocza Art. 29, Wytyczne w sprawie zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania do celów rozporządzenia 2016/679/UE (WP251rev.01), zatwierdzone przez EROD, s. 13.
[34] Świadczenie usług online może również wymagać uwzględnienia dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/770 z dnia 20 maja 2019 r. w sprawie niektórych aspektów umów o dostarczanie treści cyfrowych i usług cyfrowych (Dz.U. L 136 z 22.05.2019, s. 1), która wejdzie w życie 1 stycznia 2022 r.

Przykład 7

Wyszukiwarka internetowa usług hotelowych online monitoruje wcześniejsze rezerwacje użytkowników w celu stworzenia profilu ich typowych wydatków. Profil ten jest następnie wykorzystywany do polecania użytkownikowi określonych hoteli przy zwracaniu wyników wyszukiwania. W takim przypadku profilowanie przeszłych zachowań i danych finansowych użytkowników nie jest obiektywnie niezbędne do wykonania umowy, tj. świadczonych usług hotelarsko-gastronomicznych w oparciu o konkretne kryteria wyszukiwania dostarczone przez użytkownika. W związku z tym art. 6 ust. 1 lit. b) nie będzie miał zastosowania do tej czynności przetwarzania.

Przykład 8

Internetowa platforma handlowa umożliwia potencjalnym nabywcom przeglądanie i nabywanie produktów. Platforma chce wyświetlać spersonalizowane sugestie dotyczące produktów, wybrane na postawie produktów wystawionych na sprzedaż uprzednio oglądanych przez potencjalnych nabywców w celu zwiększenia interakcji. Personalizacja ta nie jest obiektywnie niezbędna do świadczenia usługi platformy handlowej. W związku z tym art. 6 ust. 1 lit. b) nie może stanowić podstawy prawnej takiego rodzaju przetwarzania danych osobowych.



Wytyczne 1/2019 dotyczące kodeksów postępowania i podmiotów monitorujących zgodnie z rozporządzeniem 2016/679

Wersja 2.0

4 czerwca 2019 r.

Wersja – przebieg

Wersja 2.0	4 czerwca 2019 r.	Przyjęcie wytycznych po konsultacjach społecznych
Wersja 1.0	12 lutego 2019 r.	Przyjęcie wytycznych na potrzeby konsultacji społecznych

Spis treści

1 WPROWADZENIE 5
1.1 Zakres niniejszych wytycznych. 6
2 DEFINICJE 7
3 CZYM SĄ KODEKSY? 7
4 JAKIE SĄ KORZYŚCI ZWIĄZANE Z KODEKSAMI? 8
5 DOPUSZCZALNOŚĆ PROJEKTU KODEKSU 11
5.1 Uzasadnienie i dokumentacja uzupełniająca 11
5.2 Przedstawiciel 12
5.3 Zakres przetwarzania 12
5.4 Terytorialny zakres stosowania 12
5.5 Przedłożenie kodeksu właściwemu organowi nadzorczemu 13
5.6 Nadzór nad mechanizmami 13
5.7 Podmiot monitorujący 13
5.8 Konsultacje 13
5.9 Przepisy krajowe 14
5.10 Język 14
5.11 Lista kontrolna 14
6 KRYTERIA ZATWIERDZANIA KODEKSÓW 14
6.1 Zaspokajanie określonej potrzeby 15
6.2 Ułatwienie skutecznego stosowania RODO 15
..... 16
6.3 Doprecyzowanie stosowania RODO 16
6.4 Zapewnienie wystarczających zabezpieczeń 17
6.5 Zapewnienie mechanizmów umożliwiających skuteczny nadzór 17
7 PRZEDŁOŻENIE, DOPUSZCZALNOŚĆ I ZATWIERDZENIE (KODEKS KRAJOWY) 18
7.1 Przedłożenie 18
7.2 Dopuszczalność kodeksu 18
7.3 Zatwierdzenie 19
8 PRZEDŁOŻENIE, DOPUSZCZALNOŚĆ I ZATWIERDZENIE (KODEKS TRANSGRANICZNY) 19
8.1 Przedłożenie 19
8.2 Dopuszczalność kodeksu 20
8.3 Współpraca 20

8.4 Odmowa ... 21
8.5 Przygotowanie do przedłożenia projektu Europejskiej Radzie Ochrony Danych ... 21
8.6 Europejska Rada Ochrony Danych ... 21
8.7 Zatwierdzenie ... 22
9 ZAANGAŻOWANIE ... 22
10 ROLA KOMISJI ... 23
11 MONITOROWANIE KODEKSU ... 23
12 WYMOGI AKREDYTACJI PODMIOTÓW MONITORUJĄCYCH ... 23
12.1 Niezależność ... 23
12.2 Konflikt interesów ... 25
12.3 Wiedza fachowa ... 25
12.4 Ustalone procedury i struktury ... 25
12.5 Przejrzyste rozpatrywanie skarg ... 26
12.6 Komunikacja z właściwym organem nadzorczym ... 27
12.7 Mechanizmy przeglądu ... 27
12.8 Status prawny ... 27
13 ZATWIERDZONE KODEKSY ... 28
14 ODWOŁYWANIE PODMIOTU MONITORUJĄCEGO ... 28
15 KODEKSY W SEKTORZE PUBLICZNYM ... 29
ZAŁĄCZNIK 1 – Rozróżnienie między kodeksami krajowymi a transgranicznymi ... 30
ZAŁĄCZNIK 2 – Wybór właściwego organu nadzorczego ... 31
ZAŁĄCZNIK 3 – Lista kontrolna przed przedłożeniem ... 32
ZAŁĄCZNIK 4 – KODEKS TRANSGRANICZNY Schemat blokowy ... 33

Europejska Rada Ochrony Danych,

uwzględniając art. 70 ust. 1 lit. n) oraz art. 40 i 41 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej „RODO"),

uwzględniając Porozumienie EOG, w szczególności załącznik XI i protokół 37 do tego Porozumienia, zmienione decyzją Wspólnego Komitetu EOG nr 154/2018 z dnia 6 lipca 2018 r.,

uwzględniając art. 12 i 22 swojego regulaminu z dnia 25 maja 2018 r.,

PRZYJMUJE NASTĘPUJĄCĄ OPINIĘ:

1 WPROWADZENIE

1. Rozporządzenie 2016/679[1] („RODO") weszło w życie 25 maja 2018 r. Jednym z głównych celów RODO jest zapewnienie jednolitego poziomu ochrony danych w całej Unii Europejskiej oraz zapobieganie rozbieżnościom hamującym swobodny przepływ danych osobowych na rynku wewnętrznym[2]. W RODO wprowadzono również zasadę rozliczalności, zgodnie z którą administratorzy danych są odpowiedzialni za przestrzeganie przepisów rozporządzenia oraz muszą być w stanie wykazać ich przestrzeganie[3]. Przepisy zawarte w art. 40 i 41 RODO w odniesieniu do kodeksów postępowania („kodeksy") stanowią praktyczny, potencjalnie opłacalny i znaczący sposób osiągnięcia wyższego poziomu spójności ochrony w zakresie praw do ochrony danych osobowych. Kodeksy mogą stanowić mechanizm umożliwiający wykazywanie zgodności z RODO[4]. W szczególności mogą one pomóc w wypełnieniu luk w procesie harmonizacji, które mogą występować między państwami członkowskimi podczas stosowania przez nie przepisów o ochronie danych osobowych[5]. Stanowią one również okazję dla konkretnych sektorów do refleksji nad wspólnymi czynnościami przetwarzania danych oraz do uzgodnienia specjalnych i praktycznych przepisów o ochronie danych, które będą odpowiadać potrzebom sektora, a także wymogom RODO[6].

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).
[2] Zob. motyw 13 RODO.
[3] Zob. art. 5 ust. 2 RODO.
[4] Zob. np. art. 24 ust. 3, art. 28 ust. 5 oraz art. 32 ust. 3. Z kodeksu postępowania mogą również korzystać podmioty przetwarzające dane, aby wykazać wystarczające gwarancje, że ich sposób przetwarzania jest zgodny z RODO (zob. art. 28 ust. 5).
[5] Zob. motywy 77, 81, 98, 99, 148, 168 oraz art. 24, 28, 35, 40, 41, 46, 57, 64, 70 RODO. Dotyczy to w szczególności przypadków, w których kodeks odnosi się do czynności przetwarzania w kilku państwach członkowskich.
[6] Kodeksy nie muszą być koniecznie ograniczone do konkretnego sektora. Na przykład kodeks może mieć zastosowanie do odrębnych sektorów, które mają wspólną czynność przetwarzania o takich samych cechach charakterystycznych i potrzebach. Jeżeli kodeks ma zastosowanie międzysektorowe, w ramach takiego kodeksu można powołać więcej niż jeden podmiot monitorujący. Jednak w takich przypadkach w kodeksie należy bardzo

2. Państwa członkowskie, organy nadzorcze, Europejska Rada Ochrony Danych („Rada") oraz Komisja Europejska („Komisja") są zobowiązane do zachęcania do sporządzania kodeksów mających pomóc we właściwym stosowaniu rozporządzenia[7]. Niniejsze wytyczne będą wspierać „twórców kodeksów" i ułatwiać im sporządzanie, zmianę lub rozszerzanie zakresu kodeksów.

1.1 Zakres niniejszych wytycznych

3. Celem niniejszych wytycznych jest zapewnienie praktycznych wskazówek i pomocy w zakresie wykładni w odniesieniu do stosowania art. 40 i 41 RODO. Ich celem jest wyjaśnienie procedur i przepisów związanych z przedkładaniem, zatwierdzaniem i publikowaniem kodeksów – zarówno na szczeblu krajowym, jak i europejskim. Mają one także na celu określenie minimalnych kryteriów wymaganych przez właściwy organ nadzorczy przed przystąpieniem do przeprowadzenia szczegółowego przeglądu i szczegółowej oceny kodeksu[8]. Ponadto mają na celu określenie czynników odnoszących się do treści, które należy wziąć pod uwagę przy ocenie, czy dany kodeks zapewnia właściwe i skuteczne stosowanie[9] RODO i się do takiego stosowania przyczynia. Co więcej, mają one określić wymogi dotyczące skutecznego monitorowania przestrzegania kodeksu[10].

4. Wytyczne te powinny również stanowić jasne ramy dla wszystkich właściwych organów nadzorczych, Rady i Komisji w celu spójnej oceny kodeksów oraz usprawnienia procedur związanych z procesem oceny. Ramy te powinny także dostarczyć większą przejrzystość, zapewniając, by twórcy kodeksów zamierzający ubiegać się o zatwierdzenie danego kodeksu doskonale znali przebieg procedury oraz rozumieli wymogi formalne i odpowiednie progi, których osiągnięcia wymaga się do zatwierdzenia kodeksu.

5. Wskazówki dotyczące kodeksów postępowania jako narzędzi do przekazywania danych zgodnie z art. 40 ust. 3 RODO zostaną uwzględnione w osobnych wytycznych, które ma wydać EROD.

6. Wszystkie wcześniej zatwierdzone kodeksy[11] będą musiały zostać poddane przeglądowi i ponownej ocenie zgodnie z wymogami RODO, a następnie ponownie przedłożone do zatwierdzenia zgodnie z wymogami określonymi w art. 40 i 41 oraz zgodnie z procedurami określonymi w niniejszym dokumencie.

wyraźnie wskazać, jaki jest zakres funkcji podmiotu monitorującego, innymi słowy poprzez określenie sektorów, w odniesieniu do których poszczególne podmioty monitorujące będą realizować swoje funkcje zgodnie z art. 41 oraz mechanizmów nadzoru dostępnych dla poszczególnych podmiotów monitorujących. W tym kontekście odpowiednie sekcje niniejszych wytycznych, w których określono obowiązki i wymogi dotyczące akredytacji w odniesieniu do podmiotów monitorujących, mają zastosowanie indywidualnie do każdego takiego podmiotu monitorującego wyznaczonego na podstawie kodeksu.

[7] Art. 40 ust. 1 RODO.

[8] Zob. art. 40 ust. 5, art. 55 ust. 1 i motyw 122 RODO.

[9] Zob. art. 40 ust. 1 i motyw 98 RODO.

[10] Zob. np. art. 41 ust. 2 i art. 41 ust. 3 RODO.

[11] Przez krajowe organy nadzorcze ds. danych albo Grupę Roboczą Art. 29, przed RODO oraz niniejszymi wytycznymi.

2 DEFINICJE

„Akredytacja" oznacza stwierdzenie, że proponowany podmiot monitorujący spełnia określone w art. 41 RODO wymogi w zakresie prowadzenia monitorowania przestrzegania kodeksu postępowania. Sprawdzenie to przeprowadza organ nadzorczy, któremu przedkłada się kodeks do zatwierdzenia (art. 41 ust. 1). Akredytacja podmiotu monitorującego ma zastosowanie wyłącznie wobec konkretnego kodeksu[12].

„Twórcy kodeksów" oznaczają zrzeszenia lub inne organy, które sporządzają kodeksy i przedkładają je do zatwierdzenia[13] oraz posiadają odpowiedni status prawny zgodnie z wymogami określonymi w kodeksie i zgodnie z prawem krajowym.

„Właściwy organ nadzorczy" oznacza organ nadzorczy będący organem właściwym zgodnie z art. 55 RODO.

„Podmiot monitorujący" oznacza organ/komitet lub szereg organów/komitetów (wewnętrznych lub zewnętrznych z perspektywy twórców kodeksów[14]), które pełnią funkcję monitorującą w celu stwierdzenia i zapewnienia przestrzegania kodeksu zgodnie z art. 41.

„Organy nadzorcze, których sprawa dotyczy" mają takie samo znaczenie jak w art. 4 pkt 22 RODO.

„Kodeks krajowy" oznacza kodeks, który obejmuje czynności przetwarzania prowadzone w obrębie jednego państwa członkowskiego.

„Kodeks transgraniczny" oznacza kodeks, który obejmuje czynności przetwarzania prowadzone w więcej niż jednym państwie członkowskim.

3 CZYM SĄ KODEKSY?

7. Kodeksy przewidziane w RODO to dobrowolne narzędzia w zakresie rozliczalności zawierające szczegółowe przepisy o ochronie danych w odniesieniu do kategorii administratorów i podmiotów przetwarzających. Mogą one stanowić użyteczne i skuteczne narzędzie w zakresie rozliczalności, zawierające szczegółowy opis najodpowiedniejszych, zgodnych z prawem i etycznych zbiorów zachowań w sektorze. Z punktu widzenia ochrony danych osobowych kodeksy mogą zatem funkcjonować jako zbiór instrukcji dla administratorów danych i podmiotów przetwarzających, którzy projektują i wdrażają zgodne z RODO czynności przetwarzania danych, nadających znaczenie operacyjne zasadom ochrony danych określonym w prawie europejskim i krajowym.

8. Organizacje gospodarcze lub podmioty reprezentujące sektor mogą tworzyć kodeksy, które pomogą sektorowi w przestrzeganiu przepisów RODO w sposób skuteczny i potencjalnie opłacalny. Jak przewidziano w niewyczerpującym wykazie zawartym w art. 40 ust. 2 RODO, kodeksy postępowania mogą obejmować w szczególności takie zagadnienia, jak:

- rzetelne i przejrzyste przetwarzanie;
- prawnie uzasadnione interesy realizowane przez administratorów w określonych kontekstach;
- zbieranie danych osobowych; pseudonimizacja danych osobowych;

[12] Podmiot monitorujący może być jednak akredytowany w odniesieniu do więcej niż jednego kodeksu, pod warunkiem że spełnia on wymogi dotyczące akredytacji.

[13] Zgodnie z motywem 98 RODO.

[14] Zob. również pkt 64–67 poniżej.

- informowanie osób fizycznych i wykonywanie przysługujących tym osobom praw;
- informowanie i ochrona dzieci (w tym sposoby pozyskiwania zgody rodziców);
- środki techniczne i organizacyjne, w tym ochrona danych już w fazie projektowania i domyślna ochrona danych, a także środki bezpieczeństwa;
- zgłaszanie naruszeń;
- przekazywanie danych poza UE; lub
- tryby rozstrzygania sporów.

9. W RODO, na mocy którego uchylono dyrektywę o ochronie danych (95/46/WE), zawarto bardziej skonkretyzowane i szczegółowe przepisy dotyczące kodeksów, wymogów, które należy spełnić, procedur związanych z uzyskaniem zatwierdzenia, a także rejestracji, publikacji i upowszechniania kodeksów po ich zatwierdzeniu. Przepisy te, w powiązaniu z niniejszymi wytycznymi, pomogą zachęcić twórców kodeksów do wnoszenia bezpośredniego wkładu w ustanawianie norm i reguł ochrony danych osobowych w odniesieniu do ich sektorów przetwarzania.

10. Należy zauważyć, że kodeksy są jednym z wielu dobrowolnych narzędzi z całego wachlarza narzędzi rozliczalności ochrony danych osobowych, jaki oferuje RODO, który obejmuje takie instrumenty, jak oceny skutków dla ochrony danych[15] i certyfikacja[16]. Stanowią one mechanizm, który można wykorzystać, aby pomóc organizacjom w wykazaniu zgodności z RODO[17].

4 JAKIE SĄ KORZYŚCI ZWIĄZANE Z KODEKSAMI?

11. Kodeksy zapewniają możliwość ustanowienia zbioru reguł, które przyczyniają się do właściwego stosowania RODO w sposób praktyczny, przejrzysty i potencjalnie opłacalny, a przy tym uwzględniający specyfikę danego sektora lub prowadzonych w danym sektorze czynności przetwarzania. W tym kontekście można opracować kodeksy dla administratorów i podmiotów przetwarzających, biorąc pod uwagę szczególny charakter przetwarzania, jakie prowadzi się w niektórych sektorach, oraz szczególne potrzeby mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw[18]. Mogą być one szczególnie istotnym i korzystnym narzędziem zarówno dla MŚP, jak i mikroprzedsiębiorstw[19], zapewniając mechanizm umożliwiający im osiągnięcie zgodności z przepisami ochrony danych w bardziej opłacalny sposób.

> Na przykład mikroprzedsiębiorstwa zaangażowane w podobną działalność badawczą w dziedzinie zdrowia mogłyby podjąć współpracę w ramach odpowiednich zrzeszeń i wspólnie opracować kodeks odnoszący się do zbierania i przetwarzania przez nie danych dotyczących zdrowia, zamiast samodzielnie prowadzić tak obszerną analizę ochrony danych. Kodeksy przyniosą korzyści również organom nadzorczym, umożliwiając im lepsze zrozumienie oraz uzyskanie wglądu w czynności przetwarzania danych w konkretnym zawodzie, konkretnej branży lub w innym sektorze .

12. Kodeksy mogą pomóc administratorom i podmiotom przetwarzającym w przestrzeganiu RODO poprzez regulację takich dziedzin, jak: rzetelne i przejrzyste przetwarzanie danych, prawnie uzasadnione interesy, środki bezpieczeństwa i ochrony danych już w fazie projektowania oraz domyślna ochrona danych, a także obowiązki administratora. Kodeksy są dostępne dla wszystkich sektorów przetwarzających dane i mogą być opracowywane w tak wąskim lub szerokim zakresie, jaki jest odpowiedni dla danego sektora[20], pod warunkiem że kodeks przyczynia się do właściwego i skutecznego stosowania RODO[21].

> Można byłoby na przykład wnioskować o zatwierdzenie zbioru przepisów określających sposób, w jaki konkretny sektor charytatywny miałby zapewniać rzetelne i przejrzyste zasady przetwarzania danych. Ewentualnie konkretny sektor charytatywny mógłby podjąć decyzję o opracowaniu kodeksu, który zawiera i właściwie stosuje wiele różnych przepisów na mocy RODO, tak aby objąć wszystkie czynności przetwarzania – od zgodnej z prawem podstawy gromadzenia danych osobowych po zawiadamianie o naruszeniu ochrony danych osobowych.

13. Kodeksy mogą zapewnić pewien stopień współregulacji oraz zmniejszyć poziom występującej czasami zależności administratorów i podmiotów przetwarzających od organów nadzorczych ds.

[15] Kodeksy postępowania i certyfikacja to dobrowolne narzędzia rozliczalności, zaś ocena skutków dla ochrony danych będzie w określonych okolicznościach obowiązkowa. Więcej informacji na temat innych narzędzi rozliczalności znajduje się na stronie internetowej EROD zawierającej ogólne wskazówki (www.edpb.europa.eu).
[16] Zob. art. 42 RODO oraz Wytyczne EROD nr 1/2018 dotyczące certyfikacji i określania kryteriów certyfikacji zgodnie z art. 42 i 43 RODO.
[17] Przestrzeganie danego kodeksu samo w sobie nie gwarantuje zgodności z RODO lub zwolnienia administratorów/podmiotów przetwarzających z sankcji lub z odpowiedzialności wynikającej z RODO.
[18] Zob. motyw 98 RODO w odniesieniu do art. 40 ust. 1. Kodeks mógłby być na przykład odpowiednio dostosowany do spełnienia potrzeb mikroprzedsiębiorstw w uzupełnieniu małych i średnich przedsiębiorstw.

[19] W szczególności w art. 40 ust. 1 RODO stwierdzono, że kodeksy mogą posłużyć jako rozwiązanie w celu zaspokojenia potrzeb takich przedsiębiorstw.
[20] W art. 40 ust. 2 RODO mowa o tym, że kodeksy są przygotowywane przez zrzeszenia reprezentujące „określone kategorie administratorów lub podmioty przetwarzające". Może to więc obejmować kodeksy międzysektorowe, jeżeli jest to wykonalne, pod warunkiem spełnienia kryteriów reprezentatywności.
[21] Z kodeksu o ścisłym ukierunkowaniu musi dostatecznie jasno wynikać dla osób, których dane dotyczą (oraz w sposób zadowalający dla organu nadzorczego), że fakt stosowania się przez administratorów/podmioty przetwarzające do kodeksu nie musi oznaczać zapewnienia zgodności z wszystkimi przepisami. Odpowiednim zabezpieczeniem w tym przypadku mogłoby być zapewnienie odpowiedniej przejrzystości w odniesieniu do zakresu kodeksu i jego ograniczenia do tych, którzy zobowiązali się do jego przestrzegania oraz do osób, których dotyczą dane.

ochrony danych, aby przedstawiały bardziej szczegółowe wytyczne dotyczące ich konkretnych czynności przetwarzania.

14. Kodeksy mogą także zapewnić pewien stopień autonomii i kontroli administratorom oraz podmiotom przetwarzającym w procesie formułowania i uzgadniania reguł najlepszych praktyk w przypadku ich danych sektorów. Mogą one zapewnić możliwość konsolidacji najlepszych praktyk w zakresie operacji przetwarzania w określonych dziedzinach. Mogą również stać się ważnym zasobem, na którym przedsiębiorstwa mogą się opierać przy rozwiązywaniu krytycznych problemów występujących w związku z ich procedurami przetwarzania, a także w celu osiągnięcia wyższego poziomu zgodności z przepisami o ochronie danych.

15. Kodeksy mogą zapewnić niezbędne zaufanie i zagwarantować pewność prawa poprzez dostarczenie praktycznych rozwiązań problemów zidentyfikowanych przez poszczególne sektory w odniesieniu do wspólnych czynności przetwarzania. Zachęcają one do opracowania wspólnego i spójnego podejścia do potrzeb danego sektora w zakresie przetwarzania danych.

16. Kodeksy mogą stanowić skuteczne narzędzie pozwalające zyskać zaufanie osób, których dane dotyczą. Mogą one odnosić się do różnych kwestii, z których wiele może wynikać z obaw społeczeństwa lub nawet obaw odczuwanych w samym sektorze, i jako takie stanowią narzędzie służące zwiększeniu przejrzystości w stosunku do osób fizycznych w związku z przetwarzaniem ich danych osobowych.

> Na przykład w kontekście przetwarzania danych dotyczących zdrowia do celów badawczych istnienie zatwierdzonego i szczegółowego kodeksu mogłoby rozwiać obawy związane z odpowiednimi środkami, które mają zostać przyjęte w celu propagowania zgodności z regułami mającymi zastosowanie do przetwarzania szczególnie chronionych informacji dotyczących zdrowia. Taki kodeks mógłby nakreślać w sposób rzetelny i przejrzysty następujące kwestie:
>
> - odpowiednie zabezpieczenia stosowane wobec informacji, które mają być udzielane osobom, których dane dotyczą;
> - odpowiednie zabezpieczenia stosowane wobec danych zbieranych od osób trzecich;
> - przekazywanie lub rozpowszechnianie danych;
> - kryteria, które należy wdrożyć w celu zapewnienia poszanowania zasady minimalizacji danych;
> - konkretne środki bezpieczeństwa;
> - odpowiednie okresy zatrzymywania danych; oraz
> - mechanizmy zarządzania danymi w przypadku wykonywania przez osoby, których dane dotyczą, przysługujących im praw (zgodnie z art. 32 i 89 RODO)

17. Kodeksy mogą się również okazać istotnym i pożytecznym mechanizmem w obszarze międzynarodowego przekazywania danych. Nowe przepisy zawarte w RODO umożliwiają osobom trzecim wyrażenie zgody na stosowanie zatwierdzonych kodeksów w celu spełnienia wymogów prawnych służących zapewnieniu odpowiednich zabezpieczeń w odniesieniu do międzynarodowego przekazywania danych osobowych do państw trzecich[22]. Ponadto takie zatwierdzone kodeksy mogą przyczynić się do propagowania i rozwijania poziomu ochrony, jaki RODO zapewnia szerszej społeczności międzynarodowej, umożliwiając jednocześnie zrównoważone i zgodne z prawem międzynarodowe przekazywanie danych osobowych. Mogą one również służyć jako mechanizm prowadzący do dalszego rozwoju i wzmacniania zaufania osób, których dane dotyczą, do przetwarzania danych poza Europejskim Obszarem Gospodarczym[23].

18. Zatwierdzone kodeksy mogą stanowić skuteczne narzędzia rozliczalności zarówno dla podmiotów przetwarzających, jak i administratorów danych. Jak wskazano w motywie 77 i art. 24 ust. 3 RODO, stosowanie zatwierdzonego kodeksu postępowania przewidziano, między innymi, jako odpowiednią metodę wykazywania przez administratorów danych lub podmioty przetwarzające przestrzegania określonych części rozporządzenia, zasad określonych w rozporządzeniu bądź całości rozporządzenia.[24] Stosowanie zatwierdzonego kodeksu postępowania będzie również czynnikiem branym pod uwagę przez organy nadzorcze przy ocenie konkretnych cech przetwarzania danych, takich jak aspekty bezpieczeństwa[25], przy ocenie skutków operacji przetwarzania w ramach oceny skutków dla ochrony danych[26] lub przy nakładaniu administracyjnej kary pieniężnej[27]. W przypadku naruszenia jednego z przepisów rozporządzenia przestrzeganie zatwierdzonego kodeksu postępowania może stanowić wskaźnik tego, w jakim stopniu należy zainterweniować za pomocą skutecznej, proporcjonalnej, odstraszającej administracyjnej kary pieniężnej lub innego środka naprawczego stosowanego przez organ nadzorczy[28].

5 DOPUSZCZALNOŚĆ PROJEKTU KODEKSU[29]

19. Istnieje szereg warunków, które należy spełnić, zanim właściwy organ nadzorczy będzie mógł dokonać pełnej oceny i pełnego przeglądu kodeksu do celów art. 40 ust. 5 RODO. Ma to na celu ułatwienie skutecznej oceny każdego projektu kodeksu. Zastosowanie mają następujące kryteria:

5.1 Uzasadnienie i dokumentacja uzupełniająca

[22] Zob. art. 40 ust. 2 lit. j) oraz art. 40 ust. 3 RODO.
[23] Rada przedstawi osobne wytyczne w odniesieniu do stosowania kodeksów jako mechanizmu ułatwiającego międzynarodowe przekazywanie danych.
[24] Zob. również art. 24 ust. 3 oraz art. 28 ust. 5 RODO.
[25] Art. 32 ust. 3 RODO.
[26] Art. 35 ust. 8 RODO.
[27] Art. 83 ust. 2 lit. j) RODO. Należy również zwrócić uwagę na stosowanie kodeksów w odniesieniu do Wytycznych WP 253/17 w sprawie stosowania i ustalania administracyjnych kar pieniężnych do celów rozporządzenia 2016/679, przyjętych przez EROD.
[28] *ibid.*
[29] Dotyczy to również wszelkich kodeksów (krajowych i transgranicznych), a także kodeksów zmienionych lub kodeksów o rozszerzonym zakresie.

20. Każdy projekt kodeksu przedkładany do zatwierdzenia musi zawierać jasne i zwięzłe uzasadnienie, w którym przedstawia się szczegółowe informacje o celu kodeksu, zakresie jego stosowania[30] oraz sposobie, w jaki ułatwi on skuteczne stosowanie przedmiotowego rozporządzenia[31]. Pomoże to w przyspieszeniu procesu i zapewnieniu wymaganej przejrzystości w odniesieniu do przedkładania kodeksów. W stosownych przypadkach należy również załączyć dokumentację uzupełniającą, która jest podstawą przedkładanego projektu kodeksu i uzasadnienia[32].

5.2 Przedstawiciel

21. Zgodnie z art. 40 ust. 2 kodeks muszą przedłożyć zrzeszenia lub konsorcja zrzeszeń bądź inne podmioty reprezentujące określone kategorie administratorów lub podmioty przetwarzające (twórcy kodeksów). Niewyczerpujący wykaz przykładowych twórców kodeksów obejmowałby: organizacje gospodarcze i zrzeszenia przedstawicielskie, organizacje sektorowe, organizacje akademickie i grupy interesów.

22. Twórcy kodeksów muszą wykazać przed właściwym organem nadzorczym, że są faktycznym organem przedstawicielskim i że potrafią zrozumieć potrzeby swoich członków, a także jasno określić czynność przetwarzania lub sektor, w odniesieniu do których kodeks ma być stosowany. W zależności od definicji i parametrów danego sektora reprezentatywność można określić między innymi na podstawie następujących elementów:

- liczby lub odsetka potencjalnych członków spośród właściwych administratorów lub podmiotów przetwarzających w danym sektorze;
- doświadczenia organu przedstawicielskiego w odniesieniu do działalności sektora i czynności przetwarzania związanych z kodeksem.

5.3 Zakres przetwarzania

23. Należy wyznaczyć zakres projektu kodeksu, który jasno i precyzyjnie określa operacje przetwarzania (lub cechy charakterystyczne przetwarzania) danych osobowych, których dotyczy, a także kategorie administratorów lub podmiotów przetwarzających, które reguluje. Zakres ten obejmuje problemy związane z przetwarzaniem, których rozwiązaniu ma służyć kodeks, oraz przedstawienie praktycznych rozwiązań.

5.4 Terytorialny zakres stosowania

24. W projekcie kodeksu należy określić, czy jest to kodeks krajowy, czy transgraniczny, oraz podać szczegółowe informacje na temat terytorialnego zakresu stosowania, wskazując wszystkie

[30] Zastosowanie mogą mieć następujące kategorie informacji, przy czym wykaz ten nie jest wyczerpujący: identyfikacja członków, czynność przetwarzania, osoby, których dane dotyczą, rodzaje danych, jurysdykcje, organy nadzorcze, których sprawa dotyczy (art. 4 pkt 22 RODO).

[31] Dokument ten umożliwia twórcom kodeksów przedstawienie uzasadnienia i podstaw do zatwierdzenia ich kodeksu. Stanowi on platformę dla twórców kodeksów do określenia stosowności zaproponowanych zabezpieczeń oraz wykazania, że proponowane mechanizmy są adekwatne do zakładanych celów.

[32] Przykłady mogą obejmować podsumowanie konsultacji, informacje dotyczące członkostwa lub badania, które wskazują na potrzebę wprowadzenia kodeksu.

właściwe jurysdykcje, w których ma być on stosowany. W przypadku kodeksów transgranicznych (jak również zmienionych kodeksów transgranicznych lub kodeksów transgranicznych o rozszerzonym zakresie) należy dołączyć wykaz organów nadzorczych, których sprawa dotyczy. W załączniku 1 przedstawiono różnicę między kodeksami krajowymi a transgranicznymi.

5.5 Przedłożenie kodeksu właściwemu organowi nadzorczemu

25. Twórcy kodeksów muszą zapewnić, aby organ nadzorczy wybrany do dokonania oceny projektu kodeksu był właściwy zgodnie z art. 55 RODO[33]. Załącznik 2 zawiera szczegółowe informacje, które mogą być pomocne dla twórców kodeksów przy wyborze właściwego organu nadzorczego w odniesieniu do kodeksu transgranicznego.

5.6 Nadzór nad mechanizmami

26. Projekt kodeksu musi zawierać propozycje mechanizmów umożliwiających monitorowanie przestrzegania jego przepisów przez zainteresowane strony, które podjęły się jego stosowania[34]. Dotyczy to zarówno kodeksów dla sektora publicznego, jak i dla sektora niepublicznego.

5.7 Podmiot monitorujący

27. W projekcie kodeksu, który obejmuje czynności przetwarzania prowadzone przez prywatne, niepubliczne organy lub podmioty, należy również wskazać podmiot monitorujący i określić mechanizmy umożliwiające temu podmiotowi wykonywanie jego zadań zgodnie z art. 41 RODO[35]. Wskazany podmiot monitorujący lub wskazane podmioty monitorujące muszą być w stanie spełnić wymogi dotyczące pełnej rozliczalności w swojej roli[36]. W tym celu podmiot lub podmioty monitorujące muszą zostać akredytowane przez właściwy organ nadzorczy zgodnie z art. 41 ust. 1 RODO[37].

5.8 Konsultacje

28. Projekt kodeksu musi zawierać informacje dotyczące zakresu przeprowadzonych konsultacji. W motywie 99 RODO wskazano, że sporządzając kodeks (bądź zmieniając lub rozszerzając jego zakres), należy konsultować się z odpowiednimi stronami, których sprawa dotyczy, w tym jeżeli jest to wykonalne, z osobami, których dane dotyczą. W związku z tym twórcy kodeksów powinni potwierdzić i wykazać przy przedkładaniu kodeksu do zatwierdzenia, że przeprowadzono właściwe konsultacje z odpowiednimi stronami, których sprawa dotyczy. W razie potrzeby obejmowałoby to informacje o innych kodeksach postępowania, którym mogą podlegać potencjalni członkowie,

[33] Art. 55 RODO stanowi, że każdy organ nadzorczy jest właściwy do wypełniania zadań i wykonywania uprawnień powierzonych mu zgodnie z rozporządzeniem na terytorium swojego państwa członkowskiego. Zob. również motyw 122 RODO.

[34] Zob. art. 40 ust. 4 RODO.

[35] Kodeks obejmujący sektor publiczny nadal będzie musiał zawierać odpowiednie mechanizmy monitorowania kodeksu.

[36] Zgodnie z art. 83 ust. 4 lit. c) RODO naruszenia obowiązków podmiotu monitorującego podlegają administracyjnej karze pieniężnej.

[37] Zob. poniższa sekcja zatytułowana „Wymogi dotyczące akredytacji podmiotów monitorujących" na stronie 23.

którzy zobowiązali się do stosowania kodeksu, oraz informację o tym, w jaki sposób ich kodeks uzupełnia inne kodeksy. Należy również określić poziom i charakter konsultacji, które odbyły się z udziałem członków, innych zainteresowanych stron i osób, których dane dotyczą, bądź zrzeszeń lub organów, które ich reprezentują[38]. W praktyce zdecydowanie zaleca się przeprowadzenie konsultacji z członkami organizacji lub organu będących twórcami kodeksu, a także uwzględnienie czynności przetwarzania prowadzonych w stosunku do klientów tych członków. Jeżeli z odpowiednimi zainteresowanymi stronami, których sprawa dotyczy, nie przeprowadzono żadnych konsultacji ze względu na brak takiej możliwości, twórca kodeksu musi wyjaśnić tę sytuację.

5.9 Przepisy krajowe

29. Twórcy kodeksów muszą przedstawić potwierdzenie, że projekt kodeksu jest zgodny z właściwymi przepisami krajowymi, w szczególności w przypadku gdy kodeks dotyczy sektora, który podlega przepisom szczególnym określonym w prawie krajowym, lub dotyczy operacji przetwarzania, które należy poddać ocenie, uwzględniając szczególne wymogi i odpowiednie zobowiązania prawne wynikające z prawa krajowego.

5.10 Język

30. Twórcy kodeksów powinni przestrzegać wymogów językowych określonych przez właściwy organ nadzorczy, któremu przedkładają swój kodeks. Ogólnie rzecz biorąc, należy przedłożyć kodeks sporządzony w języku właściwego organu nadzorczego danego państwa członkowskiego[39]. W przypadku kodeksów transgranicznych należy przedłożyć kodeks w języku właściwego organu nadzorczego oraz w języku angielskim[40].

5.11 Lista kontrolna

31. Ostatecznie to wybrany właściwy organ nadzorczy określi, czy projekt kodeksu przejdzie do następnego etapu oceny, tj. etapu, w ramach którego właściwy organ nadzorczy zobowiązuje się przeprowadzić pełną ocenę treści zgodnie z art. 40 i 41 RODO oraz procedurami określonymi poniżej. Listę kontrolną przedstawioną w załączniku 3 należy stosować w celu odniesienia do dokumentów przedkładanych właściwemu organowi nadzorczemu oraz jako pomoc w opracowaniu ram składania projektu kodeksu.

6 KRYTERIA ZATWIERDZANIA KODEKSÓW

32. Twórcy kodeksów będą musieli wykazać, w jaki sposób ich kodeks przyczyni się do właściwego stosowania RODO, biorąc pod uwagę szczególne cechy różnych sektorów dokonujących przetwarzania oraz szczególne wymogi i obowiązki administratorów lub podmiotów przetwarzających, których dotyczy kodeks. Istnieje szereg aspektów tego nadrzędnego wymogu. Twórcy kodeksów powinni być w stanie wykazać, że ich projekt kodeksu:

- zaspokaja określoną potrzebę danego sektora dokonującego przetwarzania lub danej czynności przetwarzania;
- ułatwia stosowanie RODO;
- doprecyzowuje stosowanie RODO;
- zapewnia wystarczające zabezpieczenia[41]; oraz
- zapewnia skuteczne mechanizmy monitorowania przestrzegania kodeksu.

6.1 Zaspokajanie określonej potrzeby

33. Twórcy kodeksów muszą wykazać, że istnieje potrzeba ustanowienia kodeksu. Kodeks jako taki musi odnosić się do problemów z ochroną danych, które pojawiają się w danym sektorze lub w przypadku określonej czynności przetwarzania.

> Na przykład sektor systemów informacyjnych wykorzystywanych do wykrywania ryzyka związanego z kredytami konsumenckimi może wskazać potrzebę opracowania kodeksu, który zapewniałby wystarczające zabezpieczenia i mechanizmy gwarantujące, by zebrane dane były istotne, prawidłowe oraz wykorzystywane wyłącznie do konkretnego, wyraźnego i prawnie uzasadnionego celu, jakim jest zapewnienie ochrony kredytowej. Podobnie sektor badań naukowych w dziedzinie zdrowia może określić potrzebę opracowania kodeksu, który zapewni spójność podejścia poprzez ustanowienie norm w celu odpowiedniego spełnienia wymogów w zakresie wyraźnej zgody i towarzyszących temu wymogów dotyczących rozliczalności na mocy RODO.

34. Twórcy kodeksu powinni być w stanie wyjaśnić i przedstawić problemy, które ma rozwiązać kodeks, i uzasadnić, w jaki sposób zapewnione dzięki kodeksowi rozwiązania będą skuteczne i korzystne nie tylko dla członków, ale również dla osób, których dane dotyczą.

6.2 Ułatwienie skutecznego stosowania RODO

35. Zgodnie z motywem 98 RODO w celu uzyskania zatwierdzenia kodeksu twórcy kodeksów będą musieli wykazać, że ich kodeks ułatwia skuteczne stosowanie RODO. W tym kontekście kodeks będzie musiał jasno określać stosowanie RODO w danym sektorze oraz określać i uwzględniać szczególne potrzeby tego sektora[42].

[38] Na przykład twórcy kodeksów mogliby przedstawić sposób, w jaki ocenili uwagi otrzymane w następstwie konsultacji.
[39] W niektórych państwach członkowskich mogą obowiązywać przepisy krajowe, zgodnie z którymi wymagane jest przedłożenie projektu kodeksu w języku narodowym; zaleca się, aby twórcy kodeksów zapytali o tę kwestię właściwy organ nadzorczy przed formalnym przedłożeniem swojego projektu kodeksu do zatwierdzenia.
[40] Zgodnie z art. 23 regulaminu wewnętrznego EROD językiem roboczym EROD jest język angielski.
[41] Oczekuje się na przykład, że w sektorach „wysokiego ryzyka", takich jak przetwarzanie danych dzieci lub danych dotyczących zdrowia, stosowane będą solidniejsze i bardziej rygorystyczne zabezpieczenia, biorąc pod uwagę wrażliwość omawianych danych osobowych.
[42] Zob. art. 40 ust. 1 RODO.

Na przykład opracowanie wykazu definicji charakterystycznych dla danego sektora oraz odpowiednie skoncentrowanie się na zagadnieniach szczególnie istotnych dla tego sektora stanowią sposoby ułatwienia skutecznego stosowania RODO. Stosowanie terminologii sektorowej, aby szczegółowo określić realizację wymogów RODO w tym sektorze może również przyczynić się do lepszego zrozumienia przepisów przez sektor i w ten sposób ułatwić skuteczne stosowanie RODO. Kodeks powinien w pełni uwzględniać prawdopodobne zagrożenia związane z czynnościami przetwarzania w konkretnym sektorze i odpowiednio dostosować powiązane obowiązki administratorów lub podmiotów przetwarzających, do których ma on zastosowanie, w świetle tych zagrożeń w danym sektorze, tj. podając przykłady dopuszczalnych zasad i warunków wykorzystania danych osobowych w marketingu bezpośrednim. Jeżeli chodzi o format, treść kodeksu należy również przedstawić w sposób ułatwiający jego zrozumienie i praktyczne stosowanie, a także skuteczne stosowanie RODO.

6.3 Doprecyzowanie stosowania RODO

36. Kodeksy będą musiały doprecyzować praktyczne stosowanie RODO i dokładnie odzwierciedlać charakter danej czynności przetwarzania lub danego sektora dokonującego przetwarzania. Powinny one zapewnić wyraźną poprawę sytuacji konkretnego sektora w odniesieniu do zgodności z prawem o ochronie danych. Kodeksy muszą także określać realistyczne i możliwe do osiągnięcia normy dla wszystkich członków oraz odznaczać się dostateczną jakością i wewnętrzną spójnością, aby zapewnić wystarczającą wartość dodaną.[43] Innymi słowy, w projekcie kodeksu należy w odpowiedni sposób skupić się na konkretnych obszarach ochrony danych[44] i kwestiach ochrony danych w sektorze, do którego ma on zastosowanie, oraz zapewnić wystarczająco jasne i skuteczne rozwiązania w odniesieniu do tych obszarów i kwestii[45].

37. Kodeks nie powinien ograniczać się do ponownego przedstawienia przepisów RODO[46]. Jego celem powinna być natomiast kodyfikacja tego, jak stosować RODO w sposób konkretny, praktyczny i precyzyjny. Uzgodnione normy i zasady będą musiały być jednoznaczne, konkretne, osiągalne i wykonalne (możliwe do sprawdzenia). Określenie odrębnych reguł w danej dziedzinie jest akceptowalną metodą, dzięki której kodeks może stanowić wartość dodaną. Stosowanie terminologii charakterystycznej jedynie dla danego sektora i przedstawianie konkretnych scenariuszy lub przykładów „najlepszych praktyk"[47] może pomóc w spełnieniu tego wymogu[48].

[43] Normę tę po raz pierwszy zastosowano w dokumencie WP 13 DG XV D/5004/98, przyjętym 10 września 1998 r.
[44] Takich jak obszary wymienione w art. 40 ust. 2 RODO.
[45] Wymóg ten odzwierciedla poprzednie stanowisko Grupy Roboczej Art. 29 przedstawione w dokumencie roboczym dotyczącym kodeksów WP 13 DG XV D/5004/98, przyjętym 10 września 1998 r.
[46] Ponowne przedstawianie przepisów o ochronie danych było stałym elementem przedłożonych projektów kodeksów, które nie zostały zatwierdzone przez Grupę Roboczą Art. 29.
[47] Oraz „niedopuszczalnych praktyk".
[48] W miarę możliwości kodeks nie powinien być napisany językiem nadmiernie prawniczym.

38. Nakreślanie planów w celu promowania zatwierdzonego kodeksu w taki sposób, aby osoby fizyczne wiedziały o jego istnieniu i treści, może również pomóc w spełnieniu normy dotyczącej „doprecyzowania stosowania RODO". Ważne jest, aby kodeksy dostarczały operacyjne znaczenie zasad ochrony danych określonych w art. 5 RODO. Istotne jest również, aby kodeksy we właściwy sposób uwzględniały odpowiednie opinie i stanowiska opublikowane lub zatwierdzone przez Radę w odniesieniu do konkretnego sektora lub konkretnej czynności przetwarzania.[49] Na przykład kodeksy zawierające specyfikacje dotyczące czynności przetwarzania mogą również ułatwić ustalenie odpowiednich podstaw prawnych tych czynności przetwarzania w państwach członkowskich, do których mają one być stosowane.

6.4 Zapewnienie wystarczających zabezpieczenia

39. Kodeks powinien również spełniać wymogi określone w art. 40 ust. 5. Zatwierdzenie zostanie wydane dopiero po ustaleniu, że projekt kodeksu zapewnia odpowiednie zabezpieczenia[50]. Twórcy kodeksu powinni w sposób zadowalający organ nadzorczy wykazać, że ich kodeks zawiera odpowiednie i skuteczne zabezpieczenia mające na celu ograniczenie ryzyka związanego z przetwarzaniem danych oraz ryzyka naruszenia praw i wolności osób fizycznych[51]. To na twórcach kodeksów będzie spoczywał obowiązek przedstawienia wyraźnych dowodów potwierdzających, że ich kodeks będzie spełniał te wymogi.

Na przykład oczekuje się, że w przypadku czynności przetwarzania „wysokiego ryzyka", takich jak przetwarzanie danych dzieci lub danych dotyczących zdrowia na dużą skalę, profilowanie lub systematyczne monitorowanie, kodeksy będą zawierały bardziej rygorystyczne wymogi dotyczące administratorów i podmiotów przetwarzających, aby zapewnić odpowiedni poziom ochrony. Ponadto korzystne dla twórców kodeksów może być przeprowadzenie szerzej zakrojonych konsultacji, zgodnie z motywem 99 RODO, w celu zapewnienia podstaw kodeksu obejmującego przetwarzanie w takich obszarach wysokiego ryzyka.

6.5 Zapewnienie mechanizmów umożliwiających skuteczny nadzór

40. Zgodnie z art. 40 ust. 4 RODO kodeks wymaga wdrożenia odpowiednich mechanizmów w celu zapewnienia, aby przestrzeganie tych przepisów było odpowiednio monitorowane oraz aby ustanowione zostały skuteczne i znaczące środki egzekucyjne w celu zapewnienia pełnej zgodności z przepisami. W kodeksie należy w szczególności określić i zaproponować struktury i procedury, które zapewnią skuteczne monitorowanie i egzekwowania naruszeń. W projekcie kodeksu należy również zidentyfikować właściwy organ, który dysponuje mechanizmami umożliwiającymi mu zapewnienie skutecznego monitorowania przestrzegania kodeksu. Mechanizmy mogą obejmować

[49] Będą one również musiały w pełni uwzględniać odpowiednie orzecznictwo krajowe i europejskie.
[50] Zob. motyw 98 RODO.
[51] Zabezpieczenia mogą również mieć zastosowanie do podmiotów monitorujących i ich zdolności do skutecznego wykonywania powierzonych im zadań.

wymogi w zakresie regularnego przeprowadzania audytów i sprawozdawczości, jasne i przejrzyste procedury rozpatrywania skarg i rozstrzygania sporów, konkretne sankcje i środki zaradcze w przypadku naruszenia przepisów kodeksu, a także zasady zgłaszania naruszeń tych przepisów.

41. Nad projektem kodeksu, który dotyczy przetwarzania prowadzonego przez niepubliczne organy i podmioty, musi czuwać podmiot monitorujący. Zasadniczo kodeks nie może uwzględniać jedynie treści przepisów mających zastosowanie do czynności przetwarzania w danym sektorze, ale musi również wdrażać mechanizmy monitorowania, które zapewnią skuteczne stosowanie tych przepisów. W projekcie kodeksu można z powodzeniem zaproponować szereg różnych mechanizmów monitorowania w sytuacjach, w których skuteczny nadzór sprawuje wiele podmiotów monitorujących. Aby zapewnić skuteczne monitorowanie kodeksu, wszystkie proponowane mechanizmy monitorowania muszą być jednak jasne, odpowiednie, osiągalne, efektywne i wykonalne (możliwe do sprawdzenia). Twórcy kodeksów będą musieli przedstawić uzasadnienie i wykazać, dlaczego ich propozycje związane z monitorowaniem są odpowiednie i możliwe do wykonania z operacyjnego punktu widzenia[52].

7 PRZEDŁOŻENIE, DOPUSZCZALNOŚĆ I ZATWIERDZENIE[53] (KODEKS KRAJOWY)

7.1 Przedłożenie

42. Twórcy kodeksu powinni oficjalnie przedłożyć jego projekt właściwemu organowi nadzorczemu w formie elektronicznej albo papierowej (w formie wydruku/na papierze)[54]. Właściwy organ nadzorczy skontaktuje się z twórcami kodeksu, potwierdzając otrzymanie projektu, i zanim przystąpi do pełnej oceny jego treści, przeprowadzi przegląd, którego celem będzie sprawdzenie, czy projekt kodeksu spełnia wspomniane wyżej kryteria dopuszczalności[55].

7.2 Dopuszczalność kodeksu

43. Jeżeli projekt kodeksu nie zostanie przyjęty ze względu na niespełnienie kryteriów dopuszczalności[56], właściwy organ nadzorczy udzieli twórcom kodeksu pisemnej odpowiedzi, przedstawiając uzasadnienie swojej decyzji. Na tej podstawie proces ten się zakończy, a od twórców kodeksu wymagać się będzie złożenia nowego projektu[57].

44. Jeżeli projekt kodeksu spełnia kryteria określone powyżej, właściwy organ nadzorczy powinien wystosować do twórców kodeksu pismo zawierające potwierdzenie, że przystąpi on do następnego etapu procesu i oceni treść projektu kodeksu zgodnie z odpowiednimi procedurami przewidzianymi w prawie krajowym.

7.3 Zatwierdzenie

45. Jeżeli na mocy prawa krajowego nie wyznaczono konkretnego terminu, właściwy organ nadzorczy powinien sporządzić opinię w rozsądnym terminie i na bieżąco przekazywać twórcom projektów informacje o postępach i orientacyjnych ramach czasowych. W opinii tej należy przedstawić uzasadnienie decyzji organu nadzorczego zgodnie z kryteriami zatwierdzania, o których mowa powyżej[58].

46. Jeżeli właściwy organ nadzorczy podejmie decyzję o odmowie zatwierdzenia, wówczas proces ten zakończy się i do twórców kodeksu należało będzie dokonanie oceny ustaleń zawartych w opinii i ponowne przemyślenie projektu kodeksu na tej podstawie. Ponadto na późniejszym etapie konieczne będzie, aby twórcy kodeksu formalnie ponownie złożyli zaktualizowany projekt kodeksu, jeżeli podejmą taką decyzję.

47. Jeżeli właściwy organ nadzorczy zatwierdzi projekt kodeksu, będzie musiał zarejestrować i opublikować kodeks (za pośrednictwem swojej strony internetowej lub innych odpowiednich metod komunikacji)[59]. W art. 40 ust. 11 zobowiązano również Radę do udostępnienia opinii publicznej wszystkich zatwierdzonych kodeksów.

8 PRZEDŁOŻENIE, DOPUSZCZALNOŚĆ I ZATWIERDZENIE[60] (KODEKS TRANSGRANICZNY)

8.1 Przedłożenie

48. Twórcy kodeksu powinni formalnie przedłożyć projekt kodeksu w formie elektronicznej albo papierowej właściwemu organowi nadzorczemu, który będzie występował jako główny organ odpowiedzialny za zatwierdzenie tego kodeksu[61]. Właściwy organ nadzorczy skontaktuje się z twórcami kodeksu, potwierdzając otrzymanie dokumentacji, i zanim przystąpi do pełnej oceny

[52] Dokument Grupy Roboczej Art. 29 pt. „Ocena samoregulacji branży: kiedy samoregulacja przyczynia się w rozsądny sposób do ochrony danych w państwie trzecim?". Dokument WP7 przyjęty dnia 14 stycznia 1998 r. jest również dokumentem informacyjnym, który umożliwia lepszy wgląd w ocenę wartości kodeksu i ogólnych podstaw koniecznych, aby zapewnić jego skuteczność. Zaleca się, aby przy opracowywaniu kodeksu (w stosownych przypadkach) wzięto pod uwagę również ten dokument.
[53] W tym zmiana i rozszerzenie zakresu uprzednio zatwierdzonych kodeksów.
[54] Takim organem będzie oczywiście krajowy organ nadzorczy dla członków, w stosunku do których kodeks ma zastosowanie. Ważne jest również, aby twórcy kodeksu wyraźnie poinformowali właściwy organ nadzorczy, że formalnie przedkładają projekt kodeksu do zatwierdzenia, oraz aby wyraźnie określili jurysdykcyjny zakres kodeksu. Należy również zwrócić uwagę na załącznik 1 w odniesieniu do różnicy między kodeksami krajowymi a transgranicznymi.
[55] Zob. również lista kontrolna w załączniku 3.
[56] *Ibid*.

[57] Warto zauważyć, że odmowa na tym etapie procesu zatwierdzania będzie się najprawdopodobniej opierała na ogólnych lub proceduralnych wymogach wstępnych, a nie na zasadniczych lub podstawowych kwestiach związanych z postanowieniami zawartymi w projekcie kodeksu.
[58] W ten sposób właściwy organ nadzorczy może zapewnić twórcom kodeksów użyteczne informacje zwrotne w przypadku, gdy zdecydują się oni na przegląd, zmianę i ponowne przedłożenie projektu kodeksu w późniejszym terminie.
[59] Zgodnie z art. 40 ust. 6 RODO.
[60] W tym zmiana i rozszerzenie zakresu uprzednio zatwierdzonych kodeksów.
[61] Kwestię tę należy interpretować w kontekście procedury opisanej poniżej.

treści, przeprowadzi przegląd, który będzie miał na celu sprawdzenie, czy projekt kodeksu spełnia wspomniane wyżej kryteria[62]. Właściwy organ nadzorczy niezwłocznie powiadomi wszystkie pozostałe organy nadzorcze o przedłożeniu kodeksu i przedstawi najważniejsze informacje, które ułatwią jego identyfikację i odniesienie się do tego kodeksu. Wszystkie organy nadzorcze powinny potwierdzić w wiadomości zwrotnej, czy są organami nadzorczymi, których sprawa dotyczy i o których mowa w art. 4 pkt 22 lit. a) i b) RODO[63].

8.2 Dopuszczalność kodeksu

49. Jeżeli projekt kodeksu nie zostanie przyjęty z powodu niespełnienia kryteriów dopuszczalności, o których mowa powyżej, właściwy organ nadzorczy zwróci się na piśmie do twórców kodeksu, przedstawiając uzasadnienie swojej decyzji. Na tej podstawie proces ten się zakończy, a od twórców kodeksu wymagać się będzie złożenia nowego projektu.[64] Właściwy organ nadzorczy wyśle również zawiadomienie, przekazując wszystkim organom nadzorczym, których sprawa dotyczy, aktualne informacje o swoim stanowisku.

50. Jeżeli właściwy organ nadzorczy zaakceptuje projekt kodeksu na podstawie spełnienia kryteriów dopuszczalności, powinien wystosować pismo do twórców kodeksu, potwierdzając, że przystąpi do następnego etapu procesu i oceni treść projektu kodeksu. Spowoduje to rozpoczęcie następującej procedury w ramach współpracy nieformalnej w odniesieniu do oceny kodeksu w celu jego zatwierdzenia.

8.3 Współpraca

51. Właściwy organ nadzorczy wyśle zawiadomienie, przekazując wszystkim organom nadzorczym[65] aktualne informacje o swoim stanowisku, wskazując organy nadzorcze, których sprawa dotyczy, i zwracając się do nich o wyznaczenie – na zasadzie dobrowolności – maksymalnie dwóch współrecenzentów, którzy pomogą w ocenie merytorycznej projektu kodeksu. Wyznaczenie współrecenzentów będzie się odbywało według kolejności zgłoszeń[66]. Zadaniem współrecenzentów będzie pomoc właściwemu organowi nadzorczemu w ocenie projektu kodeksu. Gdy wyznaczenie współrecenzentów zostanie potwierdzone, w ciągu trzydziestu dni od momentu potwierdzenia, że zostali wyznaczeni na współrecenzentów, powinni oni przekazać swoje uwagi na

[62] Zob. również lista kontrolna w załączniku 3.
[63] Kwestia ta jest istotna, gdyż przewiduje się, że współrecenzentami projektu kodeksu będą organy nadzorcze, których dotyczy przetwarzanie danych osobowych, ponieważ administrator lub podmiot przetwarzający posiadają jednostkę organizacyjną na terytorium państwa członkowskiego tego organu nadzorczego bądź ponieważ „przetwarzanie znacznie wpływa lub może znacznie wpłynąć na osoby, których dane dotyczą, mające miejsce zamieszkania w państwie członkowskim tego organu nadzorczego".
[64] Warto zauważyć, że odmowa na tym etapie procesu zatwierdzania będzie się najprawdopodobniej opierała na ogólnych lub proceduralnych wymogach wstępnych, a nie na zasadniczych lub podstawowych kwestiach związanych z przekazaniem projektu kodeksu.
[65] Organy nadzorcze, których sprawa dotyczy, powinny być możliwe do zidentyfikowania na podstawie zakresu projektu kodeksu.
[66] Wniosek ten pozostanie otwarty przez dziesięć dni roboczych. Po zidentyfikowaniu współrecenzentów właściwy organ nadzorczy przystąpi do oceny. Co do zasady w przypadku gdy kodeks będzie dotyczył co najmniej 14 państw członkowskich, właściwy organ nadzorczy skonsultuje się z dwoma współrecenzentami. Poniżej tego progu istnieje możliwość współpracy z jednym współrecenzentem lub dwoma współrecenzentami – w zależności od konkretnego przypadku.

temat treści kodeksu. Uwagi te rozpatrzy następnie właściwy organ nadzorczy podczas przeprowadzania oceny koniecznej do zatwierdzenia. Zgodnie z art. 40 ust. 7 RODO właściwy organ nadzorczy dokona ostatecznego ustalenia, czy projekt decyzji należy przedłożyć Radzie, zgodnie z art. 63 i 64 RODO[67].

52. Właściwy organ nadzorczy powinien dążyć do podjęcia decyzji w rozsądnym terminie i do regularnego przekazywania twórcom kodeksów aktualnych informacji dotyczących postępów oraz orientacyjnych ram czasowych. Powinien przedstawić uzasadnienie swojej decyzji (odmowy lub zatwierdzenia kodeksu) zgodnie z ogólnymi zasadami zatwierdzania i powiadomić o tej decyzji twórców kodeksów w odpowiednim terminie.

8.4 Odmowa

53. Jeżeli decyzja podjęta przez właściwy organ nadzorczy zakłada odmowę przekazania projektu kodeksu Radzie, proces ten zakończy się, a w gestii twórców kodeksu będzie leżała analiza ustaleń wynikających z tej decyzji i ponowne rozważenie wprowadzenia poprawek do projektu kodeksu. Ponadto na późniejszym etapie konieczne będzie, aby twórcy kodeksu formalnie ponownie złożyli projekt kodeksu, jeśli podejmą taką decyzję. Właściwy organ nadzorczy powinien również poinformować wszystkie organy nadzorcze, których sprawa dotyczy, o swoim stanowisku i przyczynach odmowy zatwierdzenia kodeksu.

8.5 Przygotowanie do przedłożenia projektu Radzie

54. Jeżeli właściwy organ nadzorczy zamierza zatwierdzić projekt kodeksu, przekaże on projekt zatwierdzenia wszystkim organom nadzorczym, których sprawa dotyczy, przed przedłożeniem projektu EROD. Wszystkie organy nadzorcze, których sprawa dotyczy, będą miały 30 dni na udzielenie odpowiedzi, a wszelkie istotne kwestie będą mogły zostać poddane pod dyskusję w odpowiedniej podgrupie EROD. Jeżeli organy nadzorcze, których sprawa dotyczy, nie udzielą odpowiedzi, rozpocznie się kolejny etap procesu prac nad kodeksem.

8.6 Europejska Rada Ochrony Danych

55. Jeżeli podjęto decyzję o skierowaniu sprawy do Rady zgodnie z art. 40 ust. 7 RODO, właściwy organ nadzorczy przekazuje tę decyzję wszystkim organom nadzorczym zgodnie z procedurą w ramach mechanizmów spójności.[68] Właściwy organ nadzorczy przekaże również sprawę Radzie zgodnie ze swoją procedurą i art. 40 ust. 7 RODO.

56. Zgodnie z art. 64 Rada wydaje opinię dotyczącą kwestii wymienionych w art. 40 ust. 7 RODO[69]. Regulamin Rady wraz z przepisami art. 64 będą miały zastosowanie do Rady i właściwego organu

[67] Może to mieć miejsce wyłącznie wówczas, gdy właściwy organ nadzorczy zamierza zatwierdzić projekt kodeksu. Zob. art. 40 ust. 7 i art. 64 ust. 1.
[68] Zob. art. 64 ust. 4 RODO, zgodnie z którym wraz z projektem decyzji właściwego organu nadzorczego należy przedstawić opinie innych organów nadzorczych, których sprawa dotyczy.
[69] Zob. zadanie Rady, o którym mowa w art. 70 ust. 1 lit. x) RODO.

nadzorczego podczas dokonywania oceny i przekazywania decyzji w sprawie zatwierdzenia kodeksów transgranicznych.

8.7 Zatwierdzenie

57. Opinia Rady zostanie przekazana właściwemu organowi nadzorczemu zgodnie z art. 64 ust. 5 RODO i do właściwego organu nadzorczego będzie należała decyzja o utrzymaniu bądź zmianie projektu decyzji zgodnie z art. 40 ust. 5[70]. Opinia Rady może zostać również przedłożona Komisji zgodnie z art. 40 ust. 8, a zgodnie z art. 40 ust. 11 Rada zgromadzi wszystkie zatwierdzone kodeksy transgraniczne i udostępni je opinii publicznej.

9 ZAANGAŻOWANIE

58. Należy zauważyć, że proces oceny nie powinien służyć jako okazja do dalszych konsultacji z właściwym organem nadzorczym w sprawie przepisów przedłożonego kodeksu. Zgodnie z art. 40 ust. 5 właściwy organ nadzorczy ma za zadanie przedstawić opinię na temat zgodności projektu kodeksu z RODO[71]. W związku z tym celem kontaktów przewidzianych między właściwym organem nadzorczym a twórcami kodeksów na tym etapie procesu będzie przede wszystkim zapewnienie wyjaśnień i pomoc podczas przeprowadzania oceny na podstawie art. 40 i 41. Przewiduje się, że w stosownych przypadkach twórcy kodeksów będą kontaktować się z organami nadzorczymi przed przedłożeniem swojego projektu kodeksu do zatwierdzenia. Co do zasady etap zatwierdzania w ramach procesu nie powinien zachęcać twórców kodeksów do dalszych konsultacji w sprawie konkretnych przepisów w projekcie kodeksu ani też umożliwiać rozszerzonej oceny, w ramach której poprawki stale przedkłada się właściwemu organowi nadzorczemu. Konieczne jest również, aby twórcy kodeksów byli dostępni w celu udzielania odpowiedzi wyjaśniających określone kwestie dotyczące ich projektu kodeksu oraz aby byli w stanie udzielić tego rodzaju odpowiedzi i wyjaśnień w rozsądnym terminie. Istotne jest, aby twórcy kodeksów byli przygotowani i zorganizowani, aby odpowiadać na zapytania w sposób efektywny i sprawny. Zaleca się, aby właściwemu organowi nadzorczemu zapewniono pojedynczy lub dedykowany punkt kontaktowy. Właściwy organ nadzorczy zdecyduje o tym, czy będzie potrzebował dodatkowych informacji przed podjęciem decyzji w sprawie projektu kodeksu, i będzie miał swobodę decydowania o sposobie komunikowania się między stronami. W celu zapewnienia ciągłości w trakcie całego procesu zatwierdzania kodeksów transgranicznych właściwy organ nadzorczy nadal będzie pełnił również funkcję głównego punktu kontaktowego.

[70] Zob. art. 64 ust. 7 i procedury, jakie przywołuje się w odniesieniu do sytuacji, gdy właściwy organ nadzorczy nie zgadza się z opinią Rady, zgodnie z art. 64 ust. 8 RODO.
[71] Właściwy organ nadzorczy może również doradzać i, w stosownych przypadkach, wydawać zalecenia dla twórców kodeksów w związku z treścią i formatem ich projektu kodeksu.

10 ROLA KOMISJI

59. W drodze aktu wykonawczego Komisja może zdecydować o powszechnym obowiązywaniu w Unii zatwierdzonego kodeksu transgranicznego i w takim przypadku zapewni jego odpowiednie upowszechnianie[72].

11 MONITOROWANIE KODEKSU

60. Aby kodeks (krajowy lub transgraniczny) został zatwierdzony, podmiot monitorujący lub podmioty monitorujące muszą zostać wskazane w kodeksie i akredytowane przez właściwy organ nadzorczy jako podmioty, które są w stanie skutecznie monitorować kodeks[73]. Zgodnie z mechanizmem spójności, o którym mowa w art. 63 RODO, właściwy organ nadzorczy przedłoży Radzie projekty wymogów dotyczących akredytacji podmiotu monitorującego. Po zatwierdzeniu przez Radę właściwy organ nadzorczy może następnie stosować te wymogi w celu akredytacji podmiotu monitorującego.

61. W RODO nie zdefiniowano terminu „akredytacja". W art. 41 ust. 2 RODO określono jednak ogólne wymogi dotyczące akredytacji podmiotu monitorującego. Istnieje szereg wymogów, które należy spełnić, aby właściwy organ nadzorczy akredytował podmiot monitorujący. Aby uzyskać akredytację, twórcy kodeksów będą musieli wyjaśnić i wykazać, w jaki sposób podmiot monitorujący, który zaproponowali, spełnia wymogi określone w art. 41 ust. 2.

62. RODO zapewnia elastyczność w odniesieniu do rodzaju i struktury podmiotu monitorującego, który ma być akredytowany zgodnie z art. 41. Twórcy kodeksów mogą zdecydować się na korzystanie z usług zewnętrznych lub wewnętrznych podmiotów monitorujących, pod warunkiem że w obu przypadkach właściwy podmiot spełnia wymogi akredytacji określone w art. 41 ust. 2, jak wskazano w liście ośmiu wymogów przedstawionych poniżej.

12 WYMOGI AKREDYTACJI PODMIOTÓW MONITORUJĄCYCH

12.1 Niezależność

63. Twórcy kodeksów będą musieli wykazać, że dany podmiot jest w odpowiedni sposób niezależny pod względem bezstronności pełnionej funkcji od członków, którzy zobowiązali się do stosowania kodeksu, oraz od przedstawicieli zawodu, branży lub sektora, do których ma zastosowanie dany kodeks. Niezależność można udowodnić w szeregu obszarów, takich jak finansowanie podmiotu

[72] Zob. art. 40 ust. 9 i art. 40 ust. 10. Taka decyzja umożliwiłaby również administratorom i podmiotom przetwarzającym, którzy nie podlegają RODO, podejmowanie wiążących i egzekwowalnych zobowiązań w odniesieniu do zatwierdzonego kodeksu (zob. art. 40 ust. 3). Umożliwiłoby to przekazywanie danych państwom trzecim lub organizacjom międzynarodowym na tej podstawie, że istnieją odpowiednie zabezpieczenia oraz że obowiązują prawa osób, których dane dotyczą, i skuteczne środki ochrony prawnej (zob. również art. 46 ust. 1 i art. 46 ust. 2 lit. e)).
[73] Art. 41 ust. 1 RODO. Należy również zauważyć, że art. 41 nie ma zastosowania do organów lub podmiotów publicznych.

monitorującego, wyznaczanie członków/pracowników, proces decyzyjny oraz – w ogólniejszym ujęciu – jego struktura organizacyjna. Poniżej omówiono te kwestie bardziej szczegółowo.

64. Istnieją dwa główne modele monitorowania, które mogą stosować twórcy kodeksów, aby spełnić wymogi dotyczące podmiotu monitorującego: zewnętrzny i wewnętrzny podmiot monitorujący. Istnieje pewien stopień elastyczności w ramach obydwu tych podejść do monitorowania i można zaproponować różne warianty, które będą odpowiednie w zależności od kontekstu danego kodeksu. Przykłady wewnętrznych podmiotów monitorujących mogłyby obejmować wewnętrzny komitet doraźny lub odrębny, niezależny departament w ramach struktury twórcy kodeksu. Obowiązkiem twórców kodeksów będzie wyjaśnienie podejścia do zarządzania ryzykiem w odniesieniu do jego bezstronności i niezależności.

65. Przykładowo w przypadku zaproponowania wewnętrznego podmiotu monitorującego należy zapewnić odrębność personelu, kierownictwa, zasad rozliczalności i funkcji od innych obszarów organizacji. Cel ten można osiągnąć na wiele sposobów, na przykład poprzez wykorzystanie skutecznych barier organizacyjnych i informacyjnych oraz odrębnych struktur zarządzania sprawozdawczością w odniesieniu do zrzeszenia i podmiotu monitorującego. Podobnie jak inspektor ochrony danych, podmiot monitorujący powinien mieć możliwość swobodnego działania bez narzuconych instrukcji i jest chroniony przed wszelkiego rodzaju sankcjami lub ingerencjami (bezpośrednimi lub pośrednimi) wynikającymi z wykonywania powierzonych zadań.

66. Niezależność może wymagać, aby doradca zewnętrzny lub inna strona, która uczestniczyła w opracowywaniu kodeksu postępowania, wykazali, że istnieją odpowiednie zabezpieczenia umożliwiające znaczne ograniczenie ryzyka dla niezależności lub ryzyka konfliktu interesów. Podmiot monitorujący musiałby przedstawić dowody potwierdzające odpowiedniość mechanizmów, które w sposób zadowalający zidentyfikują i złagodzą takie ryzyko[74]. Konieczne będzie, aby podmiot monitorujący na bieżąco identyfikował ryzyko dla swojej bezstronności, takie jak ryzyko wynikające z prowadzonej działalności lub z utrzymywanych stosunków. W przypadku stwierdzenia ryzyka dla bezstronności podmiot monitorujący powinien wykazać, w jaki sposób eliminuje takie ryzyko lub je ogranicza i w jaki sposób stosuje odpowiedni mechanizm zapewniający bezstronność.

67. Niezależność można również wykazać poprzez zademonstrowanie pełnej autonomii w zarządzaniu budżetem i innymi zasobami, w szczególności w przypadku wewnętrznego podmiotu monitorującego. Podmiot monitorujący musi również być w stanie działać w sposób niezależny przy wyborze i stosowaniu sankcji wobec administratora lub podmiotu przetwarzającego, którzy przestrzegają kodeksu. Co do zasady organ – wewnętrzny albo zewnętrzny – będzie musiał działać niezależnie od twórców kodeksów i członków, którzy zobowiązali się do stosowania kodeksu, zarówno wykonując swoje zadania, jak i korzystając ze swoich uprawnień.

[74] Podejście, jakie należy przyjąć, określi kontekst danego kodeksu. Wystarczająca może być na przykład propozycja, w przypadku której istnieje odpowiedni podział obowiązków, w ramach którego pracownicy podmiotu monitorującego nie sporządzali kodeksu, nie wykonywali jego pilotażu ani nie przeprowadzali testów dotyczących kodeksu.

12.2 Konflikt interesów[75]

68. Należy wykazać, że wykonywanie zadań i obowiązków podmiotu monitorującego nie powoduje konfliktu interesów. Twórcy kodeksów będą musieli zatem wykazać, że proponowany podmiot monitorujący powstrzyma się od wszelkich czynności niezgodnych ze swoimi zadaniami i obowiązkami oraz że wprowadzono zabezpieczenia w celu zapewnienia, aby podmiot ten nie podejmował żadnego zajęcia niezgodnego z tymi zadaniami i obowiązkami. Podmiot monitorujący musi także pozostać wolny od bezpośrednich i pośrednich wpływów zewnętrznych oraz nie zwraca się o instrukcje do żadnej osoby, organizacji ani do żadnego zrzeszenia ani ich od nich nie przyjmuje. Podmiot ten powinien posiadać własny personel, wybrany przez siebie lub przez inny podmiot niezwiązany kodeksem, który to personel powinien działać pod wyłącznym kierownictwem tych podmiotów. Wewnętrzny podmiot monitorujący chroniony jest przed wszelkiego rodzaju sankcjami lub ingerencjami (zarówno bezpośrednimi, jak i pośrednimi) twórcy kodeksu, innych właściwych organów[76] lub członków, którzy zobowiązali się do stosowania kodeksu, w związku z wykonywaniem powierzonych zadań.

12.3 Wiedza fachowa

69. Twórcy kodeksów muszą być w stanie wykazać, że podmiot monitorujący posiada wymagany poziom wiedzy fachowej do pełnienia powierzonej funkcji w skuteczny sposób. W związku z tym przedłożone dokumenty muszą zawierać szczegółowe informacje dotyczące wiedzy i doświadczenia podmiotu w zakresie prawa o ochronie danych osobowych, a także konkretnego sektora lub konkretnej czynności przetwarzania. Na przykład możliwość wykazania wcześniejszego doświadczenia w monitorowaniu danego sektora może pomóc w spełnieniu tego wymogu. Mile widziany będzie podmiot mogący wykazać się dogłębnym zrozumieniem kwestii ochrony danych oraz posiadający wiedzę ekspercką na temat konkretnych czynności przetwarzania uregulowanych w kodeksie. Personel proponowanego podmiotu monitorującego powinien również posiadać odpowiednie doświadczenie operacyjne i przeszkolenie w zakresie monitorowania zgodności, na przykład w obszarach działań związanych z audytem, monitorowaniem lub zapewnianiem jakości.

12.4 Ustalone procedury i struktury

70. Podmiot monitorujący będzie również musiał dysponować należytymi strukturami i procedurami zarządzania, które pozwolą mu odpowiednio:

- ocenić, czy administratorzy i podmioty przetwarzające kwalifikują się do stosowania kodeksu;
- monitorować zgodność działań z przepisami; oraz
- przeprowadzać przeglądy funkcjonowania kodeksu.

71. Należy opracować kompleksowe procedury weryfikacji, które pomagałyby właściwie oceniać, czy administratorzy i podmioty przetwarzające kwalifikują się do przyjęcia kodeksu oraz jego przestrzegania. Podmiot powinien również zapewnić, by przepisy kodeksu były możliwe do przestrzegania przez administratorów i podmioty przetwarzające.

[75] Bezstronność funkcji, tj. zdolność do działania w sposób niezależny.
[76] Podmioty reprezentujące kategorie administratorów lub podmiotów przetwarzających.

72. Wymagane będą procedury i struktury umożliwiające aktywne i skuteczne monitorowanie przestrzegania przepisów kodeksu przez członków, którzy zobowiązali się do jego stosowania. Mogą one obejmować wyrywkowe lub niezapowiedziane audyty, inspekcje roczne, regularne składanie sprawozdań oraz stosowanie kwestionariuszy. [77] Procedury monitorowania mogą być opracowywane na różne sposoby, o ile uwzględniają takie czynniki, jak ryzyko wynikające z przetwarzania danych w zakresie przewidzianym przez kodeks, otrzymane skargi lub szczególne incydenty, liczba członków, którzy zobowiązali się do stosowania kodeksu itp. Można byłoby rozważyć publikację sprawozdań z audytów, a także ustalenia z okresowych sprawozdań administratorów i podmiotów przetwarzających – w zakresie przewidzianym przez kodeks.

73. Twórcy kodeksów będą również musieli wykazać, że proponowany podmiot monitorujący dysponuje odpowiednimi zasobami i odpowiednim personelem, aby wykonywać swoje zadania we właściwy sposób. Zasoby powinny być proporcjonalne do oczekiwanej liczby i oczekiwanego rozmiaru członków, którzy zobowiążą się do stosowania kodeksu, a także do stopnia złożoności odpowiedniego przetwarzania danych lub stopnia ryzyka związanego z tym przetwarzaniem.

12.5 Przejrzyste rozpatrywanie skarg

74. Podmiot monitorujący będzie musiał ustanowić skuteczne procedury i struktury, które umożliwią rozpatrywanie skarg w sposób bezstronny i przejrzysty. W związku z tym musi on ustanowić publicznie dostępną procedurę rozpatrywania skarg, którego zasoby będą wystarczające do zarządzania skargami i zapewnienia, aby decyzje podmiotu były podawane do wiadomości publicznej.

> Dowodem posiadania procedury rozpatrywania skarg mógłby być na przykład opisany proces przyjmowania, oceny, śledzenia, rejestrowania i rozpatrywania skarg. Aspekty te mogłyby zostać określone w dostępnych publicznie wskazówkach dotyczących kodeksu, tak aby skarżący mógł zrozumieć procedurę rozpatrywania skarg i działać zgodnie z jej zasadami. Ponadto do niezależności takich procedur mogłyby przyczyniać się osobny personel operacyjny i osobne funkcje zarządcze w ramach podmiotu monitorującego.

75. Podmioty monitorujące powinny również posiadać skuteczne procedury zapewniające przestrzeganie kodeksu przez administratorów lub podmioty przetwarzające. Przykładem może być przyznanie podmiotowi monitorującemu uprawnienia do zawieszenia członkostwa lub wykluczenia z członkostwa administratora lub podmiotu przetwarzającego, jeżeli narusza on przepisy kodeksu (tj. środki naprawcze).

76. Jeżeli członek, który zobowiązał się do stosowania kodeksu, narusza zasady kodeksu, podmiot monitorujący ma obowiązek bezzwłocznego zastosowania odpowiednich środków. Celem odpowiednich środków naprawczych będzie powstrzymanie naruszenia i uniknięcie jego ponownego wystąpienia w przyszłości. Takie działania naprawcze i sankcje mogłyby obejmować tego rodzaju środki – począwszy od szkolenia, przez wystosowanie ostrzeżenia, zgłoszenie członka do Rady, formalne wezwanie do wdrożenia konkretnych działań w wyznaczonym terminie i tymczasowe zawieszenie członkostwa członka, który zobowiązał się do stosowania kodeksu, do czasu podjęcia działań naprawczych, aż po jego ostateczne wykluczenie z członkostwa. Środki te mogłyby zostać podane do wiadomości publicznej przez podmiot monitorujący, w szczególności w przypadku poważnych naruszeń kodeksu.

77. W razie potrzeby podmiot monitorujący powinien mieć możliwość bezzwłocznego poinformowania członka, który zobowiązał się do stosowania kodeksu, twórcy kodeksu, właściwego organu nadzorczego i wszystkich organów nadzorczych, których sprawa dotyczy, o zastosowanych środkach i ich uzasadnieniu[78]. Ponadto w przypadku gdy można zidentyfikować wiodący organ nadzorczy członka[79], który zobowiązał się do stosowania kodeksu transgranicznego, podmiot monitorujący powinien również odpowiednio poinformować ten organ o swoich działaniach.

12.6 Komunikacja z właściwym organem nadzorczym

78. Proponowane ramy podmiotu monitorującego muszą uwzględniać skuteczne przekazywanie informacji właściwemu organowi nadzorczemu i innym organom nadzorczym na temat wszelkich działań prowadzonych przez podmiot monitorujący w odniesieniu do kodeksu. Informacje te mogą obejmować decyzje dotyczące działań podejmowanych w przypadku naruszenia kodeksu przez członka, który zobowiązał się do jego stosowania, przedstawianie okresowych sprawozdań dotyczących kodeksu bądź informacje uzyskane w ramach przeglądu kodeksu lub ustalenia z jego audytu[80].

79. Ponadto podmiot ten będzie musiał zapewniać, aby organ nadzorczy pełnił swoją rolę w sposób obiektywny i niezakłócony. Na przykład kodeks, w którym proponuje się, aby członkowie mogli jednostronnie zatwierdzić, odwołać lub zawiesić podmiot monitorujący bez zawiadomienia właściwego organu nadzorczego i bez zgody tego organu, byłby sprzeczny z art. 41 ust. 5 RODO.

12.7 Mechanizmy przeglądu

80. Kodeks będzie musiał określać odpowiednie mechanizmy przeglądu w celu zagwarantowania, aby pozostał on aktualny i nadal przyczyniał się do właściwego stosowania RODO. Mechanizmy przeglądu należy wdrożyć również w celu dostosowania kodeksu do wszelkich zmian w zakresie stosowania i wykładni przepisów lub też w przypadku nowych osiągnięć technologicznych, które mogą mieć wpływ na przetwarzanie danych przez członków lub na przepisy kodeksu.

12.8 Status prawny

[77] Mogłoby się to przyczynić do zapobieżenia sytuacji, w której niektórzy członkowie są ciągle kontrolowani, zaś inni nie są poddawani kontroli.

[78] Jeżeli monitorowanie prowadzi podmiot spoza zrzeszenia/organu przedkładającego kodeks postępowania, należy poinformować o tych działaniach także twórcę kodeksu.
[79] Zgodnie z art. 56 RODO.
[80] Zob. art. 41 ust. 4.

81. Proponowany podmiot monitorujący (wewnętrzny lub zewnętrzny) oraz powiązane struktury zarządzania należy ukształtować w taki sposób, aby twórcy kodeksów byli w stanie wykazać, że podmiot monitorujący posiada odpowiednią zdolność do pełnienia swojej roli zgodnie z art. 41 ust. 4 i może podlegać karze pieniężnej zgodnie z art. 83 ust. 4 lit. c) RODO.

13 ZATWIERDZONE KODEKSY

82. Charakter i treść kodeksu określą oczywiście role odpowiednich zainteresowanych stron w zapewnianiu przestrzegania kodeksu i RODO. Właściwy organ nadzorczy będzie jednak nadal pełnił rolę polegającą na zapewnianiu, aby kodeks pozostał odpowiedni do wyznaczonego celu.

83. W związku z tym właściwy organ nadzorczy będzie ściśle współpracował z podmiotem monitorującym w zakresie wymogów dotyczących sprawozdawczości wynikających z kodeksu. Podmiot monitorujący będzie pełnił rolę głównego punktu kontaktowego oraz koordynatora w odniesieniu do wszelkich kwestii, które mogą się pojawić w związku z kodeksem.

84. Właściwy organ nadzorczy zatwierdzałby również wszelkie dalsze zmiany lub rozszerzenia zakresu kodeksu i akredytowałby wszelkie nowe podmioty monitorujące.[81] Zgodnie z art. 40 ust. 5 RODO wszelkie projekty zmian lub rozszerzenia zakresu już obowiązującego kodeksu także należy przedłożyć właściwemu organowi nadzorczemu zgodnie z procedurami określonymi w niniejszym dokumencie.

14 ODWOŁYWANIE PODMIOTU MONITORUJĄCEGO

85. W przypadku gdy podmiot monitorujący nie przestrzega obowiązujących przepisów RODO, właściwy organ nadzorczy będzie również uprawniony do cofnięcia akredytacji podmiotu monitorującego zgodnie z art. 41 ust. 5[82]. Ważne, aby twórca kodeksu zawarł w kodeksie odpowiednie przepisy dotyczące postępowania w przypadku odwołania.

86. Konsekwencje cofnięcia akredytacji jedynego podmiotu monitorującego związanego z danym kodeksem mogą jednak skutkować zawieszeniem stosowania lub trwałym wycofaniem tego kodeksu ze względu na utratę wymaganej funkcji monitorowania zgodności. Może to negatywnie wpłynąć na reputację lub interesy handlowe członków, którzy zobowiązali się do stosowania kodeksu, i może prowadzić do obniżenia poziomu zaufania osób, których dane dotyczą, lub innych zainteresowanych stron.

[81] Zmiany wymagające zatwierdzenia mogą obejmować na przykład wprowadzenie nowego przepisu do kodeksu; nie dotyczyłyby one jednak aktualizacji odniesienia do nazwy organizacji lub innych drobnych zmian, które nie mają wpływu na funkcjonowanie kodeksu.

[82] W odniesieniu do kodeksów transgranicznych ważne jest również, by właściwy organ nadzorczy zapewniał, aby wszystkie organy nadzorcze, których sprawa dotyczy, były świadome podjęcia takiego działania. Podobnie w przypadku takich kodeksów organ nadzorczy, którego sprawa dotyczy, powinien również informować właściwy organ nadzorczy, gdy okazuje się, że administrator danych (który ma przyjąć kodeks) nie przestrzega przepisów kodeksu, ponieważ takie ustalenie może wzbudzić wątpliwości co do skuteczności podmiotu monitorującego i kodeksu.

87. Jeżeli pozwalają na to okoliczności, cofnięcie akredytacji powinno nastąpić dopiero po uprzednim umożliwieniu podmiotowi monitorującemu niezwłocznego rozwiązania problemów lub wprowadzenia odpowiednich ulepszeń zgodnie z ustalonym harmonogramem przez właściwy organ nadzorczy. W przypadkach, które dotyczą kodeksów transgranicznych, przed uzgodnieniem z podmiotem monitorującym szczegółów rozwiązania stwierdzonych problemów, właściwy organ nadzorczy powinien skontaktować się w tej sprawie z organami nadzorczymi, których sprawa dotyczy. Decyzję o odwołaniu podmiotu monitorującego należy również przekazać wszystkim organom nadzorczym, których sprawa dotyczy, oraz Radzie (do celów art. 40 ust. 11).

15 KODEKSY W SEKTORZE PUBLICZNYM

88. Art. 41 ust. 6 RODO stanowi, że monitorowanie zatwierdzonych kodeksów postępowania nie będzie miało zastosowania do przetwarzania prowadzonego przez organy lub podmioty publiczne[83]. Co do zasady przepis ten uchyla wymóg monitorowania kodeksu przez akredytowany podmiot. Wyjątek ten nie pomniejsza w żaden sposób znaczenia wymogu wdrożenia skutecznych mechanizmów monitorowania kodeksu. Cel ten można osiągnąć poprzez dostosowanie obowiązujących wymogów w zakresie audytu, tak aby obejmowały one monitorowanie kodeksu.

W imieniu Europejskiej Rady Ochrony Danych

Przewodnicząca

(Andrea Jelinek)

[83] Klasyfikacja organów lub podmiotów sektora publicznego leży w gestii poszczególnych państw członkowskich.

ZAŁĄCZNIK 1 – ROZRÓŻNENIE MIĘDZY KODEKSAMI KRAJOWYMI A TRANSGRANICZNYMI

„Kodeks transgraniczny" odnosi się do kodeksu, który dotyczy czynności przetwarzania prowadzonych w więcej niż jednym państwie członkowskim. W związku z tym kodeks transgraniczny może dotyczyć czynności przetwarzania prowadzonych przez wielu administratorów lub wiele podmiotów przetwarzających w kilku państwach członkowskich, co niekoniecznie oznacza „transgraniczne przetwarzanie" zgodnie z definicją zawartą w art. 4 pkt 23 RODO.

W związku z tym w przypadku gdy kodeks postępowania przyjęty przez zrzeszenie krajowe w jednym państwie członkowskim obejmuje czynności przetwarzania prowadzone przez członków w kilku państwach członkowskich, kwalifikuje się on jako kodeks transgraniczny.

Jeżeli do zrzeszenia posiadającego kodeks zatwierdzony na poziomie krajowym przystępuje członek międzynarodowy prowadzący działalność w zakresie transgranicznego przetwarzania, członek ten może korzystać z zatwierdzonego kodeksu jedynie w odniesieniu do czynności przetwarzania w państwie członkowskim, które zatwierdziło ten kodeks[84]. Należałoby wprowadzić mechanizmy zapewniające odpowiednią przejrzystość w odniesieniu do faktycznego terytorialnego zakresu stosowania kodeksu.

[84] W powyższym przykładzie twórcy kodeksu mieliby jednak również możliwość rozważenia rozszerzenia zakresu stosowania kodeksu i ubiegania się o zatwierdzenie kodeksu transgranicznego.

ZAŁĄCZNIK 2 – WYBÓR WŁAŚCIWEGO ORGANU NADZORCZEGO

Twórcy kodeksów mogą mieć wybór w zakresie wskazania właściwego organu nadzorczego do celów ubiegania się o zatwierdzenie projektu kodeksu transgranicznego[85]. W RODO nie określono szczegółowych zasad wyznaczania właściwego organu nadzorczego, który jest najodpowiedniejszy do przeprowadzenia oceny projektu kodeksu. Aby jednak pomóc twórcom kodeksów we wskazaniu właściwego organu nadzorczego najodpowiedniejszego do dokonania oceny ich kodeksu, niektóre z czynników, które można uwzględnić, mogą obejmować[86]:

- lokalizację o największej intensywności czynności przetwarzania lub działalności sektora dokonującego przetwarzania;
- lokalizację o największym zagęszczeniu osób, których dane dotyczą i na które wpływa dana czynność przetwarzania lub dany sektor dokonujący przetwarzania;
- lokalizację siedziby twórcy kodeksu;
- lokalizację proponowanej siedziby podmiotu monitorującego; lub
- inicjatywy opracowane przez organ nadzorczy w konkretnej dziedzinie[87].

Chociaż czynniki te nie są obligatoryjnymi kryteriami, decyzja o wyborze właściwego organu nadzorczego jest istotna, a przy jej podejmowaniu należy kierować się rozsądkiem[88]. Rola właściwego organu nadzorczego obejmuje między innymi działanie jako pojedynczy punkt kontaktowy w kontaktach z twórcami kodeksów podczas procesu zatwierdzania, zarządzanie procedurą składania wniosków na etapie współpracy, akredytację podmiotu monitorującego (w stosownych przypadkach) oraz pełnienie funkcji wiodącego organu nadzorczego w celu zapewnienia skutecznego monitorowania zatwierdzonego kodeksu.

[85] Zob. art. 55 w związku z motywem 122 RODO.
[86] Wykaz ten ma charakter niewyczerpujący i niehierarchiczny.
[87] Na przykład organ nadzorczy mógł opublikować szczegółowy i istotny dokument programowy, który bezpośrednio odnosi się do czynności przetwarzania będącej przedmiotem kodeksu.
[88] Właściwy organ nadzorczy nie może odmówić przyjęcia projektu kodeksu do zatwierdzenia w oparciu o fakt, że nie spełnia on żadnego kryterium lub spełnia tylko niektóre kryteria, które wymieniono w niewyczerpującym wykazie kryteriów zawartym w załączniku 2. Odmowa może nastąpić wyłącznie na podstawie niespełnienia kryteriów określonych w sekcji zatytułowanej „Dopuszczalność projektu kodeksu".

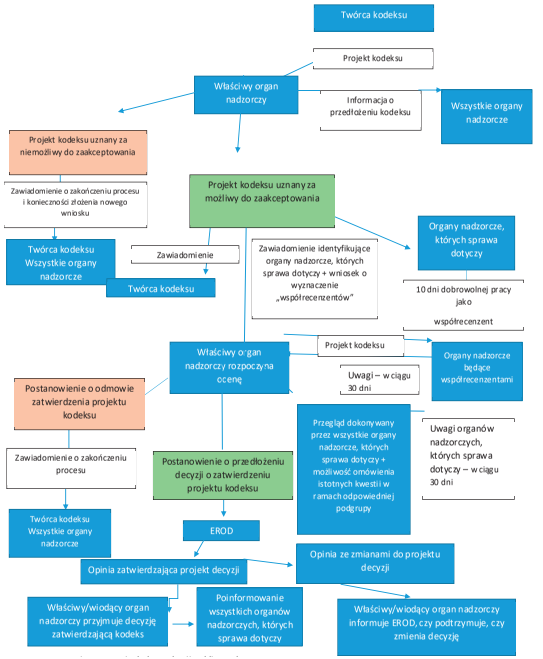
ZAŁĄCZNIK 3 – LISTA KONTROLNA PRZED PRZEDŁOŻENIEM

Przed przedłożeniem właściwemu organowi nadzorczemu projektu kodeksu należy się upewnić, że następujące elementy (w stosownych przypadkach) zostały przedłożone/wyszczególnione oraz odpowiednio oznakowane w dokumentacji:

1. Czy przedstawili Państwo uzasadnienie oraz wszelkie odpowiednie dokumenty potwierdzające? (pkt 20)
2. Czy przedkładają Państwo projekt jako zrzeszenie lub inny podmiot reprezentujący kategorie administratorów lub podmioty przetwarzające? (pkt 21)
3. Czy przedstawili Państwo szczegółowe informacje potwierdzające, że są Państwo faktycznym organem przedstawicielskim, który potrafi zrozumieć potrzeby swoich członków? (pkt 22)
4. Czy jasno określili Państwo czynność przetwarzania lub sektor dokonujący przetwarzania oraz problemy związane z przetwarzaniem, które ma rozwiązać kodeks? (pkt 23)
5. Czy określili Państwo terytorialny zakres stosowania kodeksu i załączyli wykaz wszystkich organów nadzorczych, których sprawa dotyczy (w stosownych przypadkach)? (pkt 24)
6. Czy przedstawili Państwo szczegółowe informacje, które uzasadniałyby wskazanie danego właściwego organu nadzorczego? (pkt 25)
7. Czy uwzględnili Państwo mechanizmy umożliwiające skuteczne monitorowanie przestrzegania kodeksu? (pkt 26)
8. Czy wskazali Państwo podmiot monitorujący i wyjaśnili, w jaki sposób będzie on spełniał wymogi w zakresie monitorowania kodeksu? (pkt 27)
9. Czy przedstawili Państwo informacje dotyczące zakresu konsultacji przeprowadzonych przy opracowywaniu kodeksu? (pkt 28)
10. Czy przedstawili Państwo potwierdzenie, że projekt kodeksu jest zgodny z prawem państwa członkowskiego (w stosownych przypadkach)? (pkt 29)
11. Czy spełnili Państwo wymogi językowe? (pkt 30)

Czy Państwa projekt zawiera wystarczająco szczegółowe informacje, aby wykazać właściwe stosowanie RODO? (pkt 32–41)

ZAŁĄCZNIK 4 – KODEKS TRANSGRANICZNY SCHEMAT BLOKOWY





Wytyczne 4/2018 w sprawie akredytacji podmiotów certyfikujących na podstawie art. 43 ogólnego rozporządzenia o ochronie danych (2016/679)

Wersja 3.0

4 czerwca 2019 r.

Translations proofread by EDPB Members.

This language version has not yet been proofread.

Historia wersji

Wersja 3.0	4 czerwca 2019 r.	Dodanie załącznika 1 (wersja 2.0 załącznika 1 przyjęta w dniu 4 czerwca 2019 r. po konsultacjach publicznych)
Wersja 2.0	4 grudnia 2018 r.	Przyjęcie wytycznych po konsultacjach publicznych. W tym samym dniu przyjęto załącznik 1 (wersja 1.0) do konsultacji publicznych
Wersja 1.0	6 lutego 2018 r.	Przyjęcie wytycznych przez Grupę Roboczą Art. 29 (wersja do konsultacji publicznych) Tę wersję zatwierdziła Europejska Rada Ochrony Danych w dniu 25 maja 2018 r.

Spis treści

1 Wprowadzenie ... 5
2 Zakres wytycznych ... 6
3 Interpretacja „akredytacji" dla celów art. 43 RODO ... 8
4 Akredytacja zgodnie z art. 43 ust. 1 RODO ... 9
4.1 Rola państw członkowskich ... 9
4.2 Interakcja z rozporządzeniem (WE) nr 765/2008 ... 9
4.3 Rola krajowej jednostki akredytującej ... 10
4.4 Rola organu nadzorczego ... 10
4.5 Organ nadzorczy działający w charakterze podmiotu certyfikującego ... 11
4.6 Wymogi w zakresie akredytacji ... 12
Załącznik 1 ... 13
0 Wstęp ... 13
1 Zakres ... 13
2 Odniesienie normatywne ... 13
3 Terminy i definicje ... 14
4 Ogólne wymogi w zakresie akredytacji ... 14
4.1 Kwestie prawne i umowne ... 14
4.1.1 Odpowiedzialność prawna ... 14
4.1.2 Umowa o certyfikacji ... 14
4.1.3 Stosowanie znaków jakości i oznaczeń w dziedzinie ochrony danych ... 15
4.2 Zarządzanie bezstronnością ... 15
4.3 Odpowiedzialność i finansowanie ... 15
4.4 Niedyskryminujące warunki ... 15
4.5 Poufność ... 15
4.6 Informacje dostępne publicznie ... 15
5 Wymogi strukturalne, art. 43 ust. 4 [„właściwa" ocena] ... 16
5.1 Struktura organizacyjna i ścisłe kierownictwo ... 16
5.2 Mechanizmy zapewnienia bezstronności ... 16
6 Wymogi dotyczące zasobów ... 16
6.1 Personel podmiotu certyfikującego ... 16
6.2 Zasoby na potrzeby oceny ... 17

7 Wymogi dotyczące procesów, art. 43 ust. 2 lit. c) i d) ... 17
7.1 Wytyczne ogólne ... 17
7.2 Wniosek ... 17
7.3 Rozpatrywanie wniosków ... 17
7.4 Ocena ... 18
7.5 Przegląd ... 18
7.6 Decyzja o certyfikacji ... 19
7.7 Dokumentacja certyfikacji ... 19
7.8 Wykaz certyfikowanych produktów ... 19
7.9 Nadzór ... 19
7.10 Zmiany mające wpływ na certyfikację ... 19
7.11 Wygaśnięcie, ograniczenie, zawieszenie lub cofnięcie certyfikacji ... 19
7.12 Ewidencja ... 20
7.13 Skargi i odwołania, art. 43 ust. 2 lit. d) ... 20
8 Wymogi dotyczące systemu zarządzania ... 20
8.1 Ogólne wymogi dotyczące systemu zarządzania ... 21
8.2 Dokumentacja systemu zarządzania ... 21
8.3 Kontrola dokumentów ... 21
8.4 Kontrola ewidencji ... 21
8.5 Przegląd systemu zarządzania ... 21
8.6 Audyty wewnętrzne ... 21
8.7 Działania naprawcze ... 21
8.8 Działania zapobiegawcze ... 21
9 Dalsze dodatkowe wymogi ... 21
9.1 Aktualizacja metod oceny ... 21
9.2 Utrzymywanie wiedzy fachowej ... 22
9.3 Zakresy odpowiedzialności i kompetencji ... 22
9.3.1 Komunikacja między podmiotem certyfikującym a jego klientami ... 22
9.3.2 Dokumentacja działalności w zakresie oceny ... 22
9.3.3 Zarządzanie rozpatrywaniem skarg ... 22
9.3.4 Zarządzanie cofaniem akredytacji ... 22

Europejska Rada Ochrony Danych

uwzględniając art. 70 ust. 1 lit. e) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE,

biorąc pod uwagę wyniki przeprowadzonych w lutym 2018 r. konsultacji publicznych w sprawie wytycznych oraz wyniki przeprowadzonych między 14 grudnia 2018 r. a 1 lutego 2019 r. konsultacji publicznych w sprawie załącznika, zgodnie z art. 70 ust. 4 ogólnego rozporządzenia o ochronie danych,

PRZYJMUJE NINIEJSZE WYTYCZNE:

1 WPROWADZENIE

1. Ogólne rozporządzenie o ochronie danych (rozporządzenie (UE) 2016/679) („RODO"), które wchodzi w życie dnia 25 maja 2018 r., zapewnia nowoczesne ramy zgodności dotyczące ochrony danych w Europie, oparte na rozliczalności i prawach podstawowych. Podstawę nowych ram stanowi szereg środków służących ułatwieniu zachowania zgodności z przepisami RODO. Obejmują one obowiązkowe wymogi w szczególnych okolicznościach (w tym wyznaczenie inspektorów ochrony danych i prowadzenie oceny skutków dla ochrony danych) i dobrowolne środki, takie jak kodeksy postępowania i mechanizmy certyfikacji.

2. W ramach ustanawiania mechanizmów certyfikacji oraz znaków jakości i oznaczeń w zakresie ochrony danych osobowych, w art. 43 ust. 1 RODO wymaga się od państw członkowskich zapewniania, aby podmioty certyfikujące dokonujące certyfikacji na podstawie art. 42 ust. 1 podlegały akredytacji właściwego organu nadzorczego lub krajowej jednostki akredytującej, lub obu tych podmiotów. Jeżeli akredytacji dokonuje krajowa jednostka akredytująca zgodnie z ISO/IEC 17065/2012, należy zastosować również dodatkowe wymogi określone przez właściwy organ nadzorczy.

3. Zrozumiałe mechanizmy certyfikacji mogą przyczynić się do poprawy przestrzegania RODO i zwiększenia przejrzystości dla osób, których dane dotyczą, oraz w relacjach między przedsiębiorcami (B2B), np. między administratorami a podmiotami przetwarzającymi. Administratorzy danych i podmioty przetwarzające dane będą korzystały z poświadczenia niezależnych stron trzecich, aby wykazać zgodność swoich operacji przetwarzania[1].

4. W tym kontekście Europejska Rada Ochrony Danych uznaje, że konieczne jest zapewnienie wytycznych dotyczących akredytacji. Szczególna wartość akredytacji oraz jej cel wynikają z tego, że stanowi ona wiarygodne stwierdzenie właściwości podmiotów certyfikujących, które pozwala na budowanie zaufania względem mechanizmu certyfikacji.

[1] Motyw 100 RODO stanowi, że ustanowienie mechanizmów certyfikacji może zwiększyć przejrzystość i poprawić przestrzeganie rozporządzenia oraz pozwolić w ten sposób osobom, których dane dotyczą, ocenić stopień ochrony danych, której podlegają stosowne produkty i usługi.

5. Celem wytycznych jest dostarczenie wskazówek dotyczących sposobu interpretowania i wdrażania przepisów art. 43 RODO. Mają one w szczególności na celu pomóc państwom członkowskim, organom nadzorczym i krajowym jednostkom akredytującym w ustanowieniu spójnego i jednolitego scenariusza odniesienia dotyczącego akredytacji podmiotów certyfikujących, które dokonują certyfikacji zgodnie z RODO.

2 ZAKRES WYTYCZNYCH

6. W niniejszych wytycznych:

- określono cel akredytacji w kontekście RODO;
- wyjaśniono dostępne sposoby akredytacji podmiotów certyfikujących zgodnie z art. 43 ust. 1 i określono główne kwestie, które należy rozważyć;
- zapewniono ramy służące ustanowieniu dodatkowych wymogów dotyczących akredytacji w sytuacjach, gdy dokonuje jej krajowa jednostka akredytująca; oraz
- zapewniono ramy służące ustanowieniu wymogów dotyczących akredytacji w sytuacjach, gdy dokonuje jej organ nadzorczy.

7. Niniejsze wytyczne nie są podręcznikiem procedur dotyczących akredytacji podmiotów certyfikujących zgodnie z RODO. Nie opracowano w nich nowych norm technicznych w zakresie akredytacji podmiotów certyfikujących do celów RODO.

8. Niniejsze wytyczne są skierowane do:

- państw członkowskich, które muszą zapewnić, aby akredytacji podmiotów certyfikujących dokonywały organ nadzorczy lub krajowa jednostka akredytująca;
- krajowych jednostek akredytujących, które dokonują akredytacji podmiotów certyfikujących na podstawie art. 43 ust. 1 lit. b);
- właściwego organu nadzorczego określającego dodatkowe wymogi oprócz wymogów zawartych w ISO/IEC 17065/2012[2], gdy akredytacji dokonuje krajowa jednostka akredytująca na podstawie art. 43 ust. 1 lit. b);
- Europejskiej Rady Ochrony Danych, która wydaje opinię na temat wymogów właściwego organu nadzorczego dotyczących akredytacji zgodnie z art. 43 ust. 3, art. 70 ust. 1 lit. p) i art. 64 ust. 1 lit. c) oraz zatwierdza takie wymogi;
- właściwego organu nadzorczego określającego wymogi dotyczące akredytacji, gdy dokonuje jej organ nadzorczy zgodnie z art. 43 ust. 1 lit. a);
- innych zainteresowanych stron, takich jak potencjalne podmioty certyfikujące lub właściciele systemów certyfikujących określający kryteria i procedury certyfikacji[3].

[2] Międzynarodowa Organizacja Normalizacyjna: ocena zgodności – wymogi dotyczące podmiotów certyfikujących produkty, procesy i usługi.

[3] Właścicielem systemu jest możliwa do zidentyfikowania organizacja, która określiła kryteria certyfikacji i wymogi, względem których dokonuje się oceny zgodności. Akredytacja dotyczy organizacji, która przeprowadza ocenę (art. 43 ust. 4) względem wymogów systemu certyfikacji i dokonuje certyfikacji (tj. podmiotu certyfikującego znanego również jako jednostka oceniająca zgodność). Organizacja dokonująca oceny może być tą samą organizacją, która opracowała system i jest jej właścicielem, mogą jednak istnieć ustalenia,

9. Definicje

10. Następujące definicje mają na celu promowanie wspólnego rozumienia podstawowych elementów procesu akredytacji. Należy je traktować jako punkty odniesienia, przy czym nie są one niepodważalne. Definicje te opierają się na istniejących ramach regulacyjnych i normach, szczególnie na odpowiednich przepisach RODO i ISO/IEC 17065/2012.

11. Do celów niniejszych wytycznych mają zastosowanie następujące definicje:

12. *akredytacja* podmiotów certyfikujących – zob. sekcja 3 dotycząca interpretacji akredytacji dla celów art. 43 RODO;

13. *dodatkowe wymogi* oznaczają wymogi ustanowione przez właściwy organ nadzorczy, względem którego dokonuje się akredytacji[4];

14. *certyfikacja* oznacza ocenę i bezstronne potwierdzenie przez stronę trzecią[5], że wykazano zgodność z kryteriami certyfikacji;

15. *podmiot certyfikujący* oznacza będący stroną trzecią[6]podmiot oceniający zgodność[7], posługujący się mechanizmami certyfikacji[8];

16. *system certyfikacji* oznacza system certyfikacji dotyczący określonych produktów, procesów i usług, względem których stosuje się te same określone wymogi, szczególne zasady i procedury[9];

17. *kryteria* lub kryteria certyfikacji oznaczają kryteria, na podstawie których dokonuje się certyfikacji (oceny zgodności)[10];

18. *krajowa jednostka akredytująca* oznacza jedyną autorytatywną jednostkę w państwie członkowskim, wyznaczoną zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (WE) nr 765/2008, udzielającą akredytacji na podstawie upoważnienia udzielonego jej przez państwo[11].

zgodnie z którymi jedna organizacja jest właścicielem systemu, inna zaś (lub kilka innych organizacji) dokonuje oceny.

[4] Artykuł 43 ust. 1, 3 i 6.

[5] Należy zauważyć, że zgodnie z ISO 17000 atestację (certyfikację) przez stronę trzecią „stosuje się względem wszystkich przedmiotów oceny zgodności" (5.5) „z wyjątkiem samych jednostek oceniających zgodność, względem których stosuje się akredytację" (5.6).

[6] Ocenę zgodności dokonywaną przez stronę trzecią przeprowadza organizacja, która jest niezależna od osoby lub organizacji zapewniającej jej przedmiot lub jest niezależna od interesów użytkownika tego przedmiotu, por. ISO 17000, 2.4.

[7] Zobacz ISO 17000, 2.5: „podmiot świadczący usługi oceny zgodności"; ISO 17011: „podmiot świadczący usługi oceny zgodności, który może być przedmiotem akredytacji"; ISO 17065, 3.12.

[8] Artykuł 42 ust. 1 i 5 RODO.

[9] Zobacz pkt 3.9 w związku z załącznikiem B do ISO 17065.

[10] Zobacz art. 42 ust. 5.

[11] Zobacz art. 2 pkt 11 rozporządzenia (WE) nr 765/2008.

3 INTERPRETACJA „AKREDYTACJI" DLA CELÓW ART. 43 RODO

19. W RODO nie uwzględniono definicji akredytacji. W art. 2 pkt 10 rozporządzenia (WE) nr 765/2008, które ustanawia ogólne wymagania w zakresie akredytacji, zdefiniowano akredytację jako

20. „poświadczenie przez krajową jednostkę akredytującą, że jednostka oceniająca zgodność spełnia wymagania określone w normach zharmonizowanych oraz – w stosownych przypadkach – wszelkie dodatkowe wymagania, w tym wymagania określone w odpowiednich systemach sektorowych konieczne do realizacji określonych czynności związanych z oceną zgodności".

21. Zgodnie z ISO/IEC 17011

22. „akredytacja to atestacja przez stronę trzecią, dotycząca jednostki oceniającej zgodność, służąca formalnemu wykazaniu jej kompetencji do wykonywania określonych zadań w zakresie oceny zgodności".

23. Artykuł 43 ust. 1 stanowi:

24. „Bez uszczerbku dla zadań i uprawnień właściwego organu nadzorczego wynikających z art. 57 i 58 podmiot certyfikujący, który dysponuje odpowiednim poziomem wiedzy fachowej w dziedzinie ochrony danych dokonuje certyfikacji i jej przedłużenia po poinformowaniu organu nadzorczego w celu umożliwienia mu w razie potrzeby wykonywania uprawnień na mocy art. 58 ust. 2 lit. h). Państwa członkowskie zapewniają akredytację tych podmiotów certyfikujących przez:

    a) organ nadzorczy właściwy zgodnie z art. 55 lub 56; lub
    b) krajową jednostkę akredytującą określoną zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (WE) nr 765/2008 – zgodnie z EN-ISO/IEC 17065/2012 – oraz zgodnie z dodatkowymi wymogami określonymi przez organ nadzorczy właściwy zgodnie z. 55 lub 56".

25. W odniesieniu do RODO wymogi w zakresie akredytacji będą zgodne z:

- ISO/IEC 17065/2012 i dodatkowymi wymogami ustanowionymi przez organ nadzorczy właściwy zgodnie z art. 43 ust. 1 lit. b), gdy akredytacji dokonuje krajowa jednostka akredytująca, oraz przez organ nadzorczy, gdy sam dokonuje akredytacji.

26. W obu przypadkach ujednolicone wymogi muszą obejmować wymogi, o których mowa w art. 43 ust. 2.

27. Europejska Rada Ochrony Danych przyznaje, że celem akredytacji jest zapewnienie autorytatywnego potwierdzenia kompetencji jednostki do wykonywania certyfikacji (działalności z zakresu oceny zgodności)[12]. W kontekście RODO akredytację rozumie się w następujący sposób:

[12] Porównaj motyw 15 rozporządzenia (WE) nr 765/2008.

28. poświadczenie[13] przez krajową jednostkę akredytującą lub organ nadzorczy, że podmiot certyfikujący[14] posiada kwalifikacje, aby dokonywać certyfikacji na podstawie art. 42 i 43 RODO, uwzględniając ISO/IEC 17065/2012 i dodatkowe wymogi ustanowione przez organ nadzorczy lub przez Radę.

4 AKREDYTACJA ZGODNIE Z ART. 43 UST. 1 RODO

29. W art. 43 ust. 1 uznaje się, że istnieje kilka możliwości dotyczących akredytacji podmiotów certyfikujących. W RODO wymaga się od organów nadzorczych i od państw członkowskich, aby zdefiniowały proces akredytacji podmiotów certyfikujących. W niniejszej sekcji określono dostępne sposoby akredytacji określone w art. 43.

4.1 Rola państw członkowskich

30. W art. 43 ust. 1 wymaga się od państw członkowskich *zapewnienia* akredytacji podmiotów certyfikujących, pozwala się jednak każdemu państwu członkowskiemu na określenie kto powinien być odpowiedzialny za dokonywanie oceny prowadzącej do akredytacji. Na podstawie art. 43 ust. 1 dostępne są trzy możliwości; akredytacji dokonuje:

1) wyłącznie organ nadzorczy na podstawie własnych wymogów;
2) wyłącznie krajowa jednostka akredytująca określona zgodnie z rozporządzeniem (WE) nr 765/2008 i na podstawie ISO/IEC 17065/2012 oraz zgodnie z dodatkowymi wymogami określonymi przez właściwy organ nadzorczy; lub
3) zarówno organ nadzorczy, jak i krajowa jednostka akredytująca (zgodnie z wszystkimi wymogami wymienionymi w pkt 2 powyżej).

31. Dane państwo członkowskie decyduje, czy czynności związanych z akredytacją dokona krajowa jednostka akredytująca, organ nadzorczy, czy oba te podmioty, w każdym wypadku powinno ono jednak zapewnić udostępnienie odpowiednich zasobów[15].

4.2 Interakcja z rozporządzeniem (WE) nr 765/2008

32. Europejska Rada Ochrony Danych zauważa, że w art. 2 pkt 11 rozporządzenia (WE) nr 765/2008 zdefiniowano krajową jednostkę akredytującą jako *„jedyną autorytatywną* jednostkę w państwie członkowskim, udzielającą akredytacji na podstawie upoważnienia udzielonego jej przez państwo".

33. Artykuł 2 pkt 11 może być postrzegany jako niespójny z art. 43 ust. 1 RODO, w którym zezwala się na akredytację przez inny podmiot niż krajowa jednostka akredytująca państwa członkowskiego. Europejska Rada Ochrony Danych uważa, że prawodawstwo UE ma na celu odstąpienie od ogólnej zasady, zgodnie z którą akredytacji może dokonać wyłącznie krajowa jednostka akredytująca, udzielając organom nadzorczym takiego samego uprawnienia dotyczącego akredytacji podmiotów certyfikujących. Artykuł 43 ust. 1 stanowi zatem *lex specialis* względem art. 2 pkt 11 rozporządzenia 765/2008.

[13] Porównaj art. 2 pkt 10 rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 765/2008 z dnia 9 lipca 2008 r. ustanawiającego wymagania w zakresie akredytacji i nadzoru rynku odnoszące się do warunków wprowadzania produktów do obrotu.
[14] Porównaj z definicją terminu „akredytacja" zgodnie z ISO 17011.
[15] Zobacz art. 4 ust. 9 rozporządzenia (WE) nr 765/2008.

4.3 Rola krajowej jednostki akredytującej

34. Artykuł 43 ust. 1 lit. b) stanowi, że krajowa jednostka akredytująca będzie dokonywała akredytacji podmiotów certyfikujących zgodnie z ISO/IEC 17065/2012 oraz zgodnie z dodatkowymi wymogami określonymi przez właściwy organ nadzorczy.

35. Dla zachowania jasności Europejska Rada Ochrony Danych zauważa, że szczególne odniesienie w art. 43 ust. 3 do „ust. 1 lit. [b])" oznacza, że zwrot „wymogi te" odnosi się do „dodatkowych wymogów" ustanowionych przez właściwy organ nadzorczy na podstawie art. 43 ust. 1 lit. b) oraz wymogów określonych w art. 43 ust. 2.

36. W procesie akredytacji krajowe jednostki akredytujące stosują dodatkowe wymogi, które mają dostarczyć organy nadzorcze.

37. Podmiot certyfikujący posiadający akredytację na podstawie ISO/IEC 17065/2012 w odniesieniu do systemów certyfikacji innych niż związane z RODO, który chce rozszerzyć zakres swojej akredytacji tak, aby obejmowała ona certyfikację wydaną zgodnie z RODO, będzie musiał spełnić dodatkowe wymogi ustanowione przez organ nadzorczy, jeżeli akredytacji dokonuje krajowa jednostka akredytująca. Jeżeli akredytację na potrzeby certyfikacji na podstawie RODO oferuje tylko właściwy organ nadzorczy, podmiot certyfikujący wnioskujący o akredytację będzie musiał spełnić wymogi określone przez odpowiedni organ nadzorczy.

4.4 Rola organu nadzorczego

38. Europejska Rada Ochrony Danych zauważa, że art. 57 ust. 1 lit. q) stanowi, że organ nadzorczy akredytuje podmiot certyfikujący na mocy art. 43 w ramach zadań organu nadzorczego zgodnych z art. 57, a art. 58 ust. 3 lit. e) stanowi, że organowi nadzorczemu przysługują uprawnienia w zakresie wydawania zezwoleń i uprawnienia doradcze w postaci akredytowania na mocy art. 43 podmiotów certyfikujących. Sformułowanie art. 43 ust. 1 zapewnia pewien stopień elastyczności a funkcję akredytującą organu nadzorczego należy postrzegać jak zadanie tylko w stosownych przypadkach. Do celów uściślenia tej kwestii można wykorzystać prawo państwa członkowskiego. W procesie akredytacji dokonywanej przez krajową jednostkę akredytującą wymaga się jednak od podmiotu certyfikującego zgodnie z art. 43 ust. 2 lit. a), aby w sposób satysfakcjonujący wykazał właściwemu organowi nadzorczemu swoją niezależność i wiedzę fachową w dziedzinie oferowanego przez nią mechanizmu certyfikacji[16].

39. Jeżeli państwo członkowskie zastrzega sobie, że podmioty certyfikujące mają być akredytowane przez organ nadzorczy, organ ten powinien ustanowić wymogi w zakresie akredytacji obejmujące wymogi wyszczególnione w art. 43 ust. 2, lecz nie ograniczające się do nich. W porównaniu z obowiązkami związanymi z akredytacją podmiotów certyfikujących przez krajowe jednostki certyfikujące, w art. 43 przewidziano mniej instrukcji dotyczących wymogów w zakresie akredytacji w przypadku, gdy dokonuje jej sam organ nadzorczy. W celu przyczynienia się do jednolitego podejścia do akredytacji kryteria akredytacji stosowane przez organ nadzorczy należy oprzeć na ISO/IEC 17065 oraz uzupełnić je dodatkowymi wymogami, które organ nadzorczy ustanawia na podstawie art. 43 ust. 1 lit. b).

[16] W dodatkowych wymogach ustanowionych przez organ nadzorczy zgodnie z art. 43 ust. 1 lit. b) należy określić wymogi dotyczące niezależności i wiedzy fachowej. Zobacz również załącznik 1 do wytycznych.

Europejska Rada Ochrony Danych zauważa, że art. 43 ust. 2 lit. a)–e) odzwierciedlają i uszczegóławiają wymogi ISO 17065, co przyczyni się do zachowania spójności.

40. Jeżeli państwo członkowskie zastrzega sobie, że podmioty certyfikujące mają być akredytowane przez krajowe jednostki akredytujące, organ nadzorczy powinien ustanowić dodatkowe wymogi uzupełniające istniejące praktyki przewidziane w rozporządzeniu (WE) nr 765/2008 (w którym art. 3–14 odnoszą się do organizacji i dokonywania akredytacji jednostek oceniających zgodność) oraz przepisy techniczne określające metody i procedury organów nadzorczych. W tym świetle w rozporządzeniu (WE) nr 765/2008 przewidziano dalsze wytyczne: w art. 2 pkt 10 zdefiniowano akredytację i odniesiono się do „zharmonizowanych norm" i „wszelkich dodatkowych wymagań, w tym wymagań określonych w odpowiednich systemach sektorowych". Wynika z tego, że dodatkowe wymogi ustanowione przez organ nadzorczy powinny obejmować szczególne wymogi i koncentrować się na ułatwieniu m.in. oceny niezależności i poziomu wiedzy fachowej w zakresie ochrony danych osobowych podmiotów certyfikujących, np. ich zdolności do oceny i certyfikacji operacji przetwarzania danych osobowych przez administratorów i podmioty przetwarzające na podstawie art. 42 ust. 1. Obejmują one kompetencje wymagane w odniesieniu do systemów sektorowych i ochrony podstawowych praw i wolności osób fizycznych, a w szczególności ich prawa do ochrony danych osobowych[17]. Załącznik do niniejszych wytycznych może być pomocny w dostarczeniu właściwym organom nadzorczym informacji niezbędnych przy ustanawianiu dodatkowych wymogów zgodnie z art. 43 ust. 1 lit. b) i art. 43 ust. 3.

41. Artykuł 43 ust. 6 stanowi, że „[o]rgan nadzorczy w łatwo dostępny sposób podaje do wiadomości publicznej wymogi, o których mowa w ust. 3 niniejszego artykułu, oraz kryteria, o których mowa w art. 42 ust. 5". W związku z tym, aby zapewnić przejrzystość, należy publikować wszystkie kryteria i wymogi zatwierdzone przez organ nadzorczy. Jeżeli chodzi o jakość i zaufanie względem podmiotów certyfikujących, byłoby pożądane, aby wszelkie wymogi dotyczące akredytacji były łatwo dostępne publicznie.

4.5 Organ nadzorczy działający w charakterze podmiotu certyfikującego

42. Artykuł 42 ust. 5 stanowi, że organ nadzorczy może dokonać certyfikacji, zgodnie z RODO nie musi być on jednak akredytowany, aby spełniał wymogi rozporządzenia (WE) nr 765/2008. Europejska Rada Ochrony Danych zauważa, że w art. 43 ust. 1 lit. a) i szczególnie w art. 58 ust. 2 lit. h), art. 58 ust. 3 lit. a), e)–f) nadaje się organom nadzorczym uprawnienia do dokonywania zarówno akredytacji, jak i certyfikacji, i jednocześnie do udzielania porad i w stosownych przypadkach cofnięcia certyfikacji lub nakazania podmiotowi certyfikującemu nieudzielania certyfikacji.

43. Mogą wystąpić sytuacje, w których stosowne lub wymagane jest rozdzielenie ról i obowiązków związanych z akredytacją i certyfikacją, np. jeżeli w państwie członkowskim współistnieją organ nadzorczy i inne podmioty certyfikujące i dokonują one certyfikacji w tym samym zakresie. Organy nadzorcze powinny zatem podjąć wystarczające działania organizacyjne, aby rozdzielić zadania na podstawie RODO w celu osadzenia i ułatwienia mechanizmów certyfikacji, przy jednoczesnym podjęciu środków ostrożności, aby uniknąć konfliktów interesów, które mogą wynikać z tych zadań. Ponadto państwa członkowskie i organy nadzorcze, opracowując krajowe prawo i procedury związane z akredytacją i certyfikacją zgodnie z RODO, powinny mieć na uwadze jednolity poziom europejski.

4.6 Wymogi w zakresie akredytacji

44. W załączniku do niniejszych wytycznych przedstawiono wskazówki dotyczące sposobu określenia dodatkowych wymogów w zakresie akredytacji. Określono w nim stosowne przepisy ujęte w RODO i zasugerowano wymogi, które organy nadzorcze i krajowe jednostki akredytujące powinny uwzględnić, aby zapewnić zgodność z przepisami RODO.

45. Jak ustalono powyżej, jeżeli podmioty certyfikujące są akredytowane przez krajową jednostkę akredytującą na podstawie rozporządzenia (WE) nr 765/2008, odpowiednią normą w zakresie akredytacji będzie ISO/IEC 17065/2012 uzupełniona dodatkowymi wymogami ustanowionymi przez organ nadzorczy. W świetle ochrony praw podstawowych na podstawie RODO, art. 43 ust. 2 odzwierciedla ogólne przepisy ISO/IEC 17065/2012. W ramach ujętych w załączniku zastosowano art. 43 ust. 2 i ISO/IEC 17065/2012 jako podstawę określenia wymogów i dodatkowych kryteriów związanych z oceną wiedzy fachowej podmiotów certyfikujących w zakresie ochrony danych oraz ich zdolności do poszanowania praw i wolności osób fizycznych w odniesieniu do przetwarzania danych osobowych, jak zagwarantowano w RODO. Europejska Rada Ochrony Danych zauważa, że koncentrują się one w szczególności na zapewnieniu, aby podmioty certyfikujące miały odpowiedni poziom wiedzy fachowej w zakresie ochrony danych zgodnie z art. 43 ust. 1.

46. Dodatkowe wymogi w zakresie akredytacji ustanowione przez organ nadzorczy będą miały zastosowanie względem wszystkich podmiotów certyfikujących zwracających się o akredytację. Jednostka akredytująca oceni, czy podmiot certyfikujący jest właściwy do dokonywania certyfikacji zgodnie z dodatkowymi wymogami i przedmiotem certyfikacji. Należy uwzględnić odniesienia do konkretnych sektorów lub obszarów certyfikacji, do których podmiot certyfikujący posiada akredytację.

47. Europejska Rada Ochrony Danych zauważa również, że w przypadku gdy inne podmioty zewnętrzne, takie jak laboratoria lub audytorzy, wykonują część elementów czynności w zakresie certyfikacji w imieniu akredytowanego podmiotu certyfikującego, poza wymogami ujętymi w ISO/IEC 17065/2012 wymagana jest również szczególna wiedza fachowa w dziedzinie ochrony danych. W takich przypadkach nie jest możliwa akredytacja takich zewnętrznych podmiotów na podstawie samego RODO. Aby zapewnić jednak odpowiednie kwalifikacje takich podmiotów do wykonywania ich działań w imieniu akredytowanych podmiotów certyfikujących, konieczne jest zapewnienie przez akredytowany podmiot certyfikujący, aby podmiot zewnętrzny również posiadał wiedzę fachową z zakresu ochrony danych wymaganą od podmiotów akredytowanych i wykazał się taką wiedzą, w odniesieniu do stosownego wykonywanego działania.

48. Ramy służące określeniu dodatkowych wymogów w zakresie akredytacji przedstawione w załączniku do niniejszych wytycznych nie są podręcznikiem procedur dotyczących procesu akredytacji dokonywanej przez krajową jednostkę akredytującą lub organ nadzorczy. Zawiera on wskazówki dotyczące struktury i metodyki, jest zatem zestawem narzędzi dla organów nadzorczych pomocnym w określeniu dodatkowych wymogów w zakresie akredytacji.

[17] Artykuł 1 ust. 2 RODO.

ZAŁĄCZNIK 1

Załącznik 1 zawiera wytyczne dotyczące określenia dodatkowych wymogów akredytacyjnych w odniesieniu do normy ISO/IEC 17065/2012, zgodnie z art. 43 ust. 1 lit. b) i art. 43 ust. 3 RODO.

W załączniku przedstawiono proponowane wymogi, które opracowuje organ nadzorczy ds. ochrony danych i które mają zastosowanie podczas akredytacji podmiotu certyfikującego przez krajową jednostkę akredytującą lub właściwy organ nadzorczy[18]. Te dodatkowe wymogi należy zgłosić Europejskiej Radzie Ochrony Danych przed ich zatwierdzeniem na podstawie art. 64 ust. 1 lit. c).

Niniejszy załącznik należy interpretować w powiązaniu z normą ISO/IEC 17065/2012. Stosowane tu numery sekcji odpowiadają numerom stosowanym w normie ISO/IEC 17065/2012. Dobrą praktyką byłoby stosowanie tego podejścia przez organy nadzorcze w ramach procedury akredytacji zgodnie z art. 43 ust. 1 lit. a), o ile jest to wykonalne. Ułatwi to akredytację zharmonizowaną na szczeblu UE.

Niezależnie od poniższych wytycznych lub braku wytycznych dotyczących jakiegokolwiek punktu normy ISO/IEC 17065/2012 właściwy organ nadzorczy może sformułować dalsze dodatkowe wymogi dotyczące tych punktów, pod warunkiem zgodności z prawem krajowym.

0 WSTĘP

[W niniejszej sekcji ujmuje się wszelkie ewentualne uzgodnione warunki współpracy między krajową jednostką akredytującą a organem nadzorczym ds. ochrony danych, np. określające, kto powinien odpowiadać za przyjmowanie wniosków lub jak zorganizować uznawanie zatwierdzonych kryteriów w ramach procesu akredytacji.]

1 ZAKRES[19]

Zakres normy ISO/IEC 17065/2012 stosuje się zgodnie z RODO. Dalsze informacje znajdują się w wytycznych w sprawie akredytacji i certyfikacji. Podczas procesu akredytacji krajowa jednostka akredytująca i właściwy organ nadzorczy powinny w swojej ocenie uwzględniać zakres mechanizmu certyfikacji (na przykład certyfikacja operacji przetwarzania w chmurze), w szczególności w odniesieniu do kryteriów, wiedzy fachowej i metodyki oceny. Szeroki zakres normy ISO/IEC 17065/2012, obejmujący produkty, procesy i usługi, nie powinien prowadzić do zaniżania ani zastępowania wymogów RODO. Na przykład mechanizm zarządzania nie może być jedynym elementem mechanizmu certyfikacji, ponieważ certyfikacja musi obejmować operacje przetwarzania danych osobowych. Zgodnie z art. 42 ust. 1 RODO certyfikacja ma zastosowanie wyłącznie do operacji przetwarzania prowadzonych przez administratorów i podmioty przetwarzające.

2 ODNIESIENIE NORMATYWNE

Przepisy RODO są nadrzędne wobec normy ISO/IEC 17065/2012. Jeżeli w wymogach dodatkowych lub w mechanizmie certyfikacji znajduje się odniesienie do innych norm ISO, należy je interpretować zgodnie z wymogami określonymi w RODO.

[18] Informacje na temat procesu zatwierdzania kryteriów certyfikacji znajdują się w sekcji 4 wytycznych dotyczących certyfikacji.
[19] Numeracja odpowiada normie ISO/IEC 17065/2012.

3 TERMINY I DEFINICJE

W kontekście niniejszego załącznika stosuje się terminy i definicje zawarte w wytycznych dotyczących akredytacji (WP 261) i certyfikacji (EROD 1/2018) i są one nadrzędne wobec definicji ISO.

4 OGÓLNE WYMOGI W ZAKRESIE AKREDYTACJI

4.1 Kwestie prawne i umowne

4.1.1 Odpowiedzialność prawna

Podmiot certyfikujący powinien zawsze być w stanie wykazać krajowej jednostce akredytującej lub właściwemu organowi nadzorczemu, że posiada aktualne procedury potwierdzające przestrzeganie obowiązków prawnych określonych w warunkach akredytacji, w tym dodatkowych wymogów dotyczących stosowania rozporządzenia (UE) 2016/679. Należy zauważyć, że ponieważ podmiot certyfikujący sam również jest administratorem lub podmiotem przetwarzającym dane, musi on być w stanie wykazać posiadanie procedur i środków zgodnych z rozporządzeniem (UE) 2016/679, szczególnie w odniesieniu do administrowania danymi osobowymi organizacji będącej klientem i ich obsługi w procesie certyfikacji.

Właściwy organ nadzorczy może dodać dalsze wymogi i procedury w celu sprawdzenia zgodności podmiotów certyfikujących z RODO przed akredytacją.

4.1.2 Umowa o certyfikacji

Minimalne wymogi dotyczące umowy o certyfikacji uzupełnia się o następujące punkty:

Podmiot certyfikujący musi wykazać, że jego umowy o certyfikacji, oprócz spełniania wymogów zawartych w normie ISO/IEC 17065/2012:

1. zobowiązują wnioskodawcę do stałego spełniania zarówno ogólnych wymogów w zakresie certyfikacji w rozumieniu pkt 4.1.2.2 lit. a) normy ISO/IEC 17065/2012, jak kryteriów zatwierdzonych przez właściwy organ nadzorczy lub EROD zgodnie z art. 43 ust. 2 lit. b) i art. 42 ust. 5;
2. zobowiązują wnioskodawcę, aby zapewnił pełną przejrzystość wobec właściwego organu nadzorczego w odniesieniu do procedury certyfikacji, w tym kwestii objętych postanowieniami umownymi o poufności, dotyczących ochrony danych, zgodnie z art. 42 ust. 7 i art. 58 ust. 1 lit. c);
3. nie ograniczają odpowiedzialności wnioskodawcy za zgodność z rozporządzeniem (UE) 2016/679 i pozostają bez uszczerbku dla zadań i uprawnień organów nadzorczych, które są właściwe na mocy art. 42 ust. 5;
4. zobowiązują wnioskodawcę do dostarczenia podmiotowi certyfikującemu wszelkich informacji i dostępu do prowadzonych przez wnioskodawcę czynności przetwarzania w zakresie niezbędnym do przeprowadzenia procedury certyfikacji zgodnie z art. 42 ust. 6;
5. zobowiązują wnioskodawcę do przestrzegania obowiązujących terminów i procedur, np. wynikających z programu certyfikacji lub innych przepisów;
6. w odniesieniu do pkt 4.1.2.2 lit. c) ppkt 1) normy ISO/IEC 17065/2012 – określają zasady ważności, przedłużenia i cofnięcia certyfikacji zgodnie z art. 42 ust. 7 i art. 43 ust. 4, w tym zasady określające odpowiednie odstępy czasu na ponowną ocenę lub przegląd (regularność) zgodnie z art. 42 ust. 7;

7. zezwalają podmiotowi certyfikującemu na ujawnienie wszelkich informacji niezbędnych do przyznania certyfikacji zgodnie z art. 42 ust. 8 i art. 43 ust. 5;
8. zawierają przepisy dotyczące niezbędnych środków ostrożności w odniesieniu do rozpatrywania skarg w rozumieniu pkt 4.1.2.2 lit. c) ppkt 2), a ponadto (lit. j)) zawierają również wyraźne oświadczenia na temat struktury i procedury rozpatrywania skarg zgodnie z art. 43 ust. 2 lit. d);
9. w uzupełnieniu minimalnych wymogów, o których mowa w pkt 4.1.2.2 normy ISO/IEC 17065/2012, w przypadku gdy skutki cofnięcia lub zawieszenia akredytacji dla podmiotu certyfikującego mają konsekwencje dla klienta, należy je również uwzględnić;
10. zobowiązują wnioskodawcę do powiadomienia podmiotu certyfikującego o ewentualnych istotnych zmianach jego sytuacji faktycznej lub prawnej oraz o zmianach produktów, procesów i usług objętych certyfikacją.

4.1.3 Stosowanie znaków jakości i oznaczeń w dziedzinie ochrony danych

Certyfikaty, znaki jakości i oznaczenia stosuje się wyłącznie w sposób zgodny z art. 42 i 43 oraz z wytycznymi w sprawie akredytacji i certyfikacji.

4.2 Zarządzanie bezstronnością

Jednostka akredytująca zapewnia, że w uzupełnieniu do wymogu określonego w sekcji 4.2 normy ISO/IEC 17065/2012:

1. jednostka certyfikująca spełnia dodatkowe wymogi określone przez właściwy organ nadzorczy (na podstawie art. 43 ust. 1 lit. b)),
   a. zgodnie z art. 43 ust. 2 lit. a) przedstawia odrębne dowody swojej niezależności, w szczególności w odniesieniu do finansowania podmiotu certyfikującego w zakresie, w jakim wiąże się to z zapewnieniem bezstronności;
   b. jej zadania i obowiązki nie prowadzą do konfliktu interesów zgodnie z art. 43 ust. 2 lit. e);
2. jednostka certyfikująca nie jest powiązana w istotny sposób z klientem, którego ocenia.

4.3 Odpowiedzialność i finansowanie

W uzupełnieniu do wymogu zawartego w pkt 4.3.1 normy ISO/IEC 17065/2012 jednostka akredytująca regularnie zapewnia, że podmiot certyfikujący posiada odpowiednie środki (np. ubezpieczenia lub rezerwy) w celu pokrycia swoich zobowiązań w regionach geograficznych, w których prowadzi działalność.

4.4 Niedyskryminujące warunki

Organ nadzorczy może sformułować dodatkowe wymogi pod warunkiem ich zgodności z prawem krajowym.

4.5 Poufność

Organ nadzorczy może sformułować dodatkowe wymogi pod warunkiem ich zgodności z prawem krajowym.

4.6 Informacje dostępne publicznie

Jednostka akredytująca, w uzupełnieniu do wymogu określonego w pkt 4.6. normy ISO/IEC 17065/2012, zobowiązuje podmiot certyfikujący co najmniej do tego, aby:

1. wszystkie (obecne i poprzednie) wersje zatwierdzonych kryteriów stosowanych w rozumieniu art. 42 ust. 5, jak również wszystkie procedury certyfikacji były opublikowane i łatwo dostępne publicznie, zasadniczo wraz z określeniem terminu ważności;
2. informacje na temat procedur rozpatrywania skarg i odwołań były podane do wiadomości publicznej zgodnie z art. 43 ust. 2 lit. d).

5 WYMOGI STRUKTURALNE, ART. 43 UST. 4 [„WŁAŚCIWA" OCENA]

5.1 Struktura organizacyjna i ścisłe kierownictwo

Organ nadzorczy może sformułować dodatkowe wymogi.

5.2 Mechanizmy zapewnienia bezstronności

Organ nadzorczy może sformułować dodatkowe wymogi.

6 WYMOGI DOTYCZĄCE ZASOBÓW

6.1 Personel podmiotu certyfikującego

Jednostka akredytująca, w uzupełnieniu do wymogu określonego w sekcji 6 normy ISO/IEC 17065/2012, zapewnia w odniesieniu do każdego podmiotu certyfikującego, że jego personel:

1. wykazał posiadanie odpowiedniej i aktualnej wiedzy i doświadczenia w zakresie ochrony danych zgodnie z art. 43 ust. 1;
2. charakteryzuje się niezależnością i dysponuje aktualną wiedzą fachową w odniesieniu do przedmiotu certyfikacji zgodnie z art. 43 ust. 2 lit. a) i nie jest w sytuacji konfliktu interesów zgodnie z art. 43 ust. 2 lit. e);
3. zobowiązuje się do przestrzegania kryteriów, o których mowa w art. 42 ust. 5, zgodnie z art. 43 ust. 2 lit. b);
4. dysponuje odpowiednią wiedzą i doświadczeniem w zakresie stosowania przepisów dotyczących ochrony danych;
5. dysponuje odpowiednią wiedzą i doświadczeniem w zakresie technicznych i organizacyjnych środków ochrony danych;
6. jest w stanie wykazać się doświadczeniem w dziedzinach wymienionych w dodatkowych wymaganiach 6.1.1, 6.1.4 i 6.1.5, a konkretnie:

pracownicy posiadający fachową wiedzę techniczną:

- posiadają kwalifikacje w odpowiedniej dziedzinie technicznej, odpowiadające co najmniej poziomowi 6 według europejskich ram kwalifikacji[20], lub uznany chroniony tytuł (np. dyplom inżynierski) w odpowiednim zawodzie regulowanym lub posiadają znaczące doświadczenie zawodowe;
- *pracownicy odpowiedzialni za decyzje w sprawie certyfikacji* muszą posiadać istotne doświadczenie zawodowe w zakresie określania i wdrażania środków ochrony danych;
- *pracownicy odpowiedzialni za ocenę* muszą posiadać doświadczenie zawodowe w zakresie technicznych środków ochrony danych oraz wiedzę i doświadczenie

[20] Zob. narzędzie do porównania ram kwalifikacji na stronie https://ec.europa.eu/ploteus/en/compare?

w zakresie porównywalnych procedur (np. certyfikacji/audytów), a w stosownych przypadkach wykazać rejestrację;

pracownicy muszą wykazać, że utrzymują wiedzę specjalistyczną w zakresie umiejętności technicznych i audytowych poprzez ustawiczne doskonalenie zawodowe;

pracownicy posiadający fachową wiedzę prawniczą:

- mają ukończone studia prawnicze na uczelni uznanej na szczeblu unijnym lub krajowym, trwające co najmniej osiem semestrów i zakończone uzyskaniem stopnia magistra prawa lub równoważnego stopnia bądź posiadają znaczące doświadczenie zawodowe;
- *pracownicy odpowiedzialni za decyzje w sprawie certyfikacji* muszą wykazać się znaczącym doświadczeniem zawodowym w zakresie prawa ochrony danych i być zarejestrowani zgodnie z wymogami państwa członkowskiego;
- *pracownicy odpowiedzialni za ocenę* muszą wykazać posiadanie co najmniej dwuletniego doświadczenia zawodowego w zakresie prawa ochrony danych oraz wiedzy i doświadczenia w zakresie porównywalnych procedur (np. certyfikacji/audytów), oraz być zarejestrowani, o ile jest to wymagane przez dane państwo członkowskie;
    - pracownicy muszą wykazać, że utrzymują wiedzę specjalistyczną w zakresie umiejętności technicznych i audytowych poprzez ustawiczne doskonalenie zawodowe.

6.2 Zasoby na potrzeby oceny

Organ nadzorczy może sformułować dodatkowe wymogi pod warunkiem ich zgodności z prawem krajowym.

7 WYMOGI DOTYCZĄCE PROCESÓW, ART. 43 UST. 2 LIT. C) I D)

7.1 Wytyczne ogólne

Jednostka akredytująca, w uzupełnieniu do wymogu określonego w sekcji 7.1 normy ISO/IEC 17065/2012, jest zobowiązana zapewnić, że:

1. podmioty certyfikujące spełniają dodatkowe wymogi właściwego organu nadzorczego (zgodnie z art. 43 ust. 1 lit. b)) przy składaniu wniosku, tak aby zadania i obowiązki nie prowadziły do powstania konfliktu interesów zgodnie z art. 43 ust. 2 lit. b);
2. powiadamiają właściwe organy nadzorcze, zanim jednostka certyfikująca zacznie działać w oparciu o zatwierdzony europejski znak jakości ochrony danych w nowym państwie członkowskim za pośrednictwem biura pomocniczego.

7.2 Wniosek

W uzupełnieniu do pkt 7.2 normy ISO/IEC 17065/2012 należy wymagać, aby:

1. przedmiot certyfikacji (przedmiot oceny) był szczegółowo opisany we wniosku wraz z interfejsami i transferami do innych systemów i organizacji, protokołów i innych gwarancji;
2. we wniosku określono, czy korzysta się z podmiotów przetwarzających, a jeżeli wnioskodawcą jest podmiot przetwarzający – aby opisano jego obowiązki i zadania oraz dołączono odnośną umowę z administratorem lub podmiotem przetwarzającym.

7.3 Rozpatrywanie wniosków

W uzupełnieniu do pkt 7.3 normy ISO/IEC 17065/2012 należy wymagać, aby:

1. w umowie o certyfikacji określone były wiążące metody oceny w odniesieniu do przedmiotu oceny;
2. w ocenie dotyczącej wystarczającej wiedzy fachowej, przewidzianej w pkt 7.3 lit. e), uwzględniano w odpowiednim zakresie zarówno techniczną, jak i prawną wiedzę fachową w zakresie ochrony danych.

7.4 Ocena

W uzupełnieniu do pkt 7.4 normy ISO/IEC 17065/2012 w mechanizmach certyfikacji należy określić wystarczające metody oceny zgodności operacji przetwarzania z kryteriami certyfikacji, w tym na przykład, w stosownych przypadkach:

1. metodę oceny konieczności i proporcjonalności operacji przetwarzania w odniesieniu do ich celu oraz osób, których dane dotyczą;
2. metodę oceny zakresu, składu i analizy wszelkiego ryzyka uwzględnionego przez administratora i podmiot przetwarzający w odniesieniu do skutków prawnych zgodnie z art. 30, 32, 35 i 36 RODO oraz w odniesieniu do definicji środków technicznych i organizacyjnych zgodnie z art. 24, 25 i 32 RODO w zakresie, w jakim wyżej wymienione artykuły mają zastosowanie do przedmiotu certyfikacji;
3. metodę oceny środków zaradczych, w tym gwarancji, zabezpieczeń i procedur służących zapewnieniu ochrony danych osobowych w kontekście operacji przetwarzania, które mają być przypisane do przedmiotu certyfikacji, oraz służących wykazaniu, że spełnione są wymogi prawne określone w kryteriach oraz
4. sposób dokumentowania metod i ustaleń.

Podmiot certyfikujący powinien być zobowiązany do zapewnienia standaryzacji i ogólnego stosowania tych metod oceny. Oznacza to stosowanie porównywalnych metod oceny do porównywalnych przedmiotów oceny. Wszelkie odstępstwa od tej procedury muszą być uzasadnione przez podmiot certyfikujący.

W uzupełnieniu do pkt 7.4.2 normy ISO/IEC 17065/2012 należy zezwolić na przeprowadzanie oceny przez ekspertów zewnętrznych uznanych przez jednostkę certyfikującą.

W uzupełnieniu do pkt 7.4.5 normy ISO/IEC 17065/2012 należy wymagać, aby certyfikacja w zakresie ochrony danych zgodna z art. 42 i 43 RODO, która obejmuje już część przedmiotu certyfikacji, mogła być włączona do bieżącej procedury certyfikacji. Nie będzie ona jednak wystarczająca do całkowitego zastąpienia (częściowych) ocen. Podmiot certyfikujący powinien być zobowiązany do sprawdzenia zgodności z kryteriami. Na potrzeby uznania należy w każdym wypadku wymagać dostępności pełnego sprawozdania z oceny lub informacji umożliwiających ocenę poprzedniej działalności w zakresie certyfikacji i jej wyników. Oświadczenie certyfikacyjne lub podobne świadectwa certyfikacji nie powinny być uznawane za wystarczające do zastąpienia sprawozdania.

W uzupełnieniu do pkt 7.4.6 normy ISO/IEC 17065/2012 należy zobowiązać podmiot certyfikujący, aby określił szczegółowo w swoim mechanizmie certyfikacji, w jaki sposób informacje wymagane w pkt 7.4.6 pozwalają klientowi (podmiotowi wnioskującemu o certyfikację) uzyskać wiedzę o niezgodnościach w odniesieniu do mechanizmu certyfikacji. W tym kontekście należy określić przynajmniej charakter i ramy czasowe takich informacji.

W uzupełnieniu do pkt 7.4.9 normy ISO/IEC 17065/2012 należy wymagać zapewnienia organowi nadzorczemu ds. ochrony danych pełnego dostępu do dokumentacji.

7.5 Przegląd

W uzupełnieniu do pkt 7.5 normy ISO/IEC 17065/2012 wymagane są procedury wydawania, regularnego przeglądu i cofania odpowiednich certyfikatów zgodnie z art. 43 ust. 2 i 3.

7.6 Decyzja o certyfikacji

W uzupełnieniu do pkt 7.6.1 normy ISO/IEC 17065/2012 podmiot certyfikujący powinien być zobowiązany do szczegółowego określenia w swoich procedurach, w jaki sposób zapewniona jest jego niezależność i odpowiedzialność w odniesieniu do poszczególnych decyzji o certyfikacji.

7.7 Dokumentacja certyfikacji

W uzupełnieniu do pkt 7.7.1 lit. e) normy ISO/IEC 17065/2012 i zgodnie z art. 42 ust. 7 RODO należy wymagać, aby okres ważności certyfikacji nie przekraczał trzech lat.

W uzupełnieniu do pkt 7.7.1 lit. e) normy ISO/IEC 17065/2012 należy wymagać, aby okres planowanego monitorowania w rozumieniu sekcji 7.9 również był dokumentowany.

W uzupełnieniu do pkt 7.7.1 lit. f) normy ISO/IEC 17065/2012 podmiot certyfikujący powinien być zobowiązany do określenia przedmiotu certyfikacji w dokumentacji certyfikacji (ze wskazaniem, w stosownych przypadkach, statusu wersji lub podobnych cech).

7.8 Wykaz certyfikowanych produktów

W uzupełnieniu do pkt 7.8 normy ISO/IEC 17065/2012 podmiot certyfikujący powinien być zobowiązany do przechowywania do wewnętrznego i publicznego wglądu informacji o certyfikowanych produktach, procesach i usługach. Podmiot certyfikujący podaje do wiadomości publicznej streszczenie sprawozdania z oceny, służące zapewnieniu przejrzystości co do przedmiotu certyfikacji i sposobu oceny. W streszczeniu przedstawia się między innymi:

a) zakres certyfikacji i miarodajny opis przedmiotu certyfikacji (przedmiotu oceny),

b) odpowiednie kryteria certyfikacji (z podaniem wersji lub statusu funkcjonalnego),

c) metody oceny i przeprowadzone badania,

d) wyniki.

W uzupełnieniu do pkt 7.8 normy ISO/IEC 17065/2012 i zgodnie z art. 43 ust. 5 RODO podmiot certyfikujący informuje właściwe organy nadzorcze o przyczynach udzielenia lub cofnięcia certyfikacji, o którą się do niego zwrócono.

7.9 Nadzór

W uzupełnieniu do pkt 7.9.1, 7.9.2 i 7.9.3 normy ISO/IEC 17065/2012 oraz zgodnie z art. 43 ust. 2 lit. c) RODO należy wprowadzić wymóg obowiązkowych regularnych środków monitorowania w celu utrzymania certyfikacji w okresie monitorowania.

7.10 Zmiany mające wpływ na certyfikację

W uzupełnieniu pkt 7.10.1 i 7.10.2 normy EN ISO/IEC 17065/2012 zmiany mające wpływ na certyfikację, które wymagają uwzględnienia przez jednostkę certyfikującą, obejmują: zmiany w przepisach prawnych dotyczących ochrony danych, przyjęcie aktów delegowanych Komisji Europejskiej zgodnie z art. 43 ust. 8 i 9, decyzje Europejskiej Rady Ochrony Danych oraz decyzje sądowe dotyczące ochrony danych. Zmiany proceduralne wymagające uwzględnienia mogą obejmować: okresy przejściowe, proces zatwierdzania przez właściwy organ nadzorczy, ponowną ocenę odnośnego przedmiotu certyfikacji oraz odpowiednie środki w celu cofnięcia certyfikacji, jeśli certyfikowana operacja przetwarzania danych nie jest już zgodna z aktualnymi kryteriami.

7.11 Wygaśnięcie, ograniczenie, zawieszenie lub cofnięcie certyfikacji

W uzupełnieniu do pkt 7.11.1 normy ISO/IEC 17065/2012 podmiot certyfikujący powinien być zobowiązany do niezwłocznego pisemnego powiadomienia właściwego organu nadzorczego oraz w stosownych przypadkach krajowej jednostki akredytującej o podjętych środkach oraz o kontynuacji, ograniczeniu, zawieszeniu lub cofnięciu certyfikacji.

Zgodnie z art. 58 ust. 2 lit. h) podmiot certyfikujący powinien być zobowiązany do przyjmowania od właściwego organu nadzorczego decyzji i zarządzeń o cofnięciu lub odmowie przyznania certyfikacji klientowi (wnioskodawcy), jeżeli wymóg certyfikacji nie został spełniony lub przestał być spełniany.

7.12 Ewidencja

Podmiot certyfikujący powinien być zobowiązany do przechowywania pełnej dokumentacji, która powinna być zrozumiała, aktualna i nadająca się do audytu.

7.13 Skargi i odwołania, art. 43 ust. 2 lit. d)

W uzupełnieniu do pkt 7.13.1 normy ISO/IEC 17065/2012 należy wymagać, aby podmiot certyfikujący określił:

a) kto może składać skargi lub zastrzeżenia,

b) kto rozpatruje skargi lub zastrzeżenia po stronie podmiotu certyfikującego,

c) jakie weryfikacje przeprowadza się w tym kontekście;

d) możliwości konsultacji z zainteresowanymi stronami.

W uzupełnieniu do pkt 7.13.2 normy ISO/IEC 17065/2012 należy wymagać, aby podmiot certyfikujący określił:

a) w jaki sposób i komu należy wydać potwierdzenie, o którym mowa,

b) terminy jego wydawania;

c) jakie procesy należy następnie uruchomić.

W uzupełnieniu do pkt 7.13.1 normy ISO/IEC 17065/2012 podmiot certyfikujący musi określić, w jaki sposób zapewniona jest odrębność rozpatrywania odwołań i skarg od czynności certyfikacyjnych.

8 WYMOGI DOTYCZĄCE SYSTEMU ZARZĄDZANIA

Zgodnie z ogólnym wymogiem dotyczącym systemu zarządzania przewidzianym w rozdziale 8 normy ISO/IEC 17065/2012 wdrażanie wszystkich wymogów zawartych w poprzednich rozdziałach w ramach stosowania mechanizmu certyfikacji przez akredytowany podmiot certyfikujący musi być dokumentowane, oceniane, kontrolowane i monitorowane w sposób niezależny

Podstawową zasadą zarządzania jest określenie systemu, w którym jego cele są ustalane skutecznie i efektywnie, co dotyczy w szczególności wdrażania usług certyfikacyjnych – na podstawie odpowiednich specyfikacji. Wymaga to przejrzystości i możliwości weryfikacji wdrożenia wymogów akredytacyjnych przez jednostkę certyfikującą oraz stałego utrzymywania zgodności z nimi.

W tym celu w systemie zarządzania należy określić metody wypełniania i kontrolowania tych wymogów zgodnie z przepisami o ochronie danych oraz metody ciągłej kontroli tych wymogów przez samą jednostkę akredytowaną.

Te zasady zarządzania i ich udokumentowane wdrażanie muszą być przejrzyste i ujawniane przez akredytowany podmiot certyfikujący w ramach procedury akredytacji zgodnie z art. 58, a następnie na wniosek organu nadzorczego ds. ochrony danych w każdym momencie podczas dochodzenia

w formie przeglądów w zakresie ochrony danych na podstawie art. 58 ust. 1 lit. b) lub przeglądu – na podstawie art. 58 ust. 1 lit. c) – certyfikacji udzielonych na mocy art. 42 ust. 7.

Akredytowana jednostka certyfikująca musi w szczególności stale podawać do wiadomości publicznej, które certyfikacje (lub mechanizmy bądź systemy certyfikacji) zostały przeprowadzone na jakiej podstawie oraz jaki jest okres ważności certyfikacji na podstawie jakich ram i warunków (motyw 100).

8.1 Ogólne wymogi dotyczące systemu zarządzania

Właściwy organ nadzorczy może określić dalsze dodatkowe wymogi pod warunkiem ich zgodności z prawem krajowym.

8.2 Dokumentacja systemu zarządzania

Właściwy organ nadzorczy może określić dalsze dodatkowe wymogi pod warunkiem ich zgodności z prawem krajowym.

8.3 Kontrola dokumentów

Właściwy organ nadzorczy może określić dalsze dodatkowe wymogi pod warunkiem ich zgodności z prawem krajowym.

8.4 Kontrola ewidencji

Właściwy organ nadzorczy może określić dalsze dodatkowe wymogi pod warunkiem ich zgodności z prawem krajowym.

8.5 Przegląd systemu zarządzania

Właściwy organ nadzorczy może określić dalsze dodatkowe wymogi pod warunkiem ich zgodności z prawem krajowym.

8.6 Audyty wewnętrzne

Właściwy organ nadzorczy może określić dalsze dodatkowe wymogi pod warunkiem ich zgodności z prawem krajowym.

8.7 Działania naprawcze

Właściwy organ nadzorczy może określić dalsze dodatkowe wymogi pod warunkiem ich zgodności z prawem krajowym.

8.8 Działania zapobiegawcze

Właściwy organ nadzorczy może określić dalsze dodatkowe wymogi pod warunkiem ich zgodności z prawem krajowym.

9 DALSZE DODATKOWE WYMOGI21

9.1 Aktualizacja metod oceny

Podmiot certyfikujący ustanawia procedury aktualizacji metod oceny stosowanych w kontekście oceny, o której mowa w pkt 7.4. Aktualizacja musi następować w kontekście zmian ram prawnych, odnośnego ryzyka, aktualnego stanu wiedzy oraz kosztów wdrożenia środków technicznych i organizacyjnych.

[21] Właściwy organ nadzorczy może określić dalsze dodatkowe wymogi pod warunkiem ich zgodności z prawem krajowym.

9.2 Utrzymywanie wiedzy fachowej

Jednostki certyfikujące ustanawiają procedury służące zapewnieniu szkolenia pracowników w celu aktualizacji ich umiejętności, z uwzględnieniem zmian, o których mowa w pkt 9.1.

9.3 Zakresy odpowiedzialności i kompetencji

9.3.1 Komunikacja między podmiotem certyfikującym a jego klientami

Zapewnia się istnienie procedur wdrażania odpowiednich procedur i struktur komunikacyjnych między podmiotem certyfikującym a klientem. Obejmują one:

1. prowadzenie przez akredytowany podmiot certyfikujący dokumentacji zadań i obowiązków do celów:
    a. odpowiadania na wnioski o udzielenie informacji lub
    b. umożliwienia kontaktu w przypadku skargi dotyczącej certyfikacji;
2. prowadzenie procesu przyjmowania wniosków w celu:
    a. udzielania informacji o postępie w rozpatrywaniu wniosku;
    b. przeprowadzania przez właściwy organ nadzorczy oceny dotyczącej:
        i. informacji zwrotnej;
        ii. decyzji właściwego organu nadzorczego.

9.3.2 Dokumentacja działalności w zakresie oceny

Organ nadzorczy może sformułować dodatkowe wymogi.

9.3.3 Zarządzanie rozpatrywaniem skarg

Rozpatrywanie skarg powinno stanowić integralną część systemu zarządzania, zgodną w szczególności z wymogami pkt 4.1.2.2 lit. c), 4.1.2.2 lit. j), 4.6 lit. d) i 7.13 normy ISO/IEC 17065/2012.

Odpowiednie skargi i sprzeciwy należy zgłaszać właściwemu organowi nadzorczemu.

9.3.4 Zarządzanie cofaniem akredytacji

Procedury w przypadku zawieszenia lub cofnięcia akredytacji włącza się do systemu zarządzania podmiotu certyfikującego, co obejmuje powiadamianie klientów.



Wytyczne 3/2018 w sprawie terytorialnego zakresu stosowania RODO (art. 3)

Wersja 2.0

12 listopada 2019 r.

Historia wersji

Wersja 2.0	12 listopada 2019 r.	Przyjęcie wytycznych po konsultacjach publicznych
Wersja 1.0	16 listopada 2018 r.	Przyjęcie wytycznych do konsultacji publicznych

Spis treści

Wprowadzenie 4

1 Stosowanie kryterium „jednostki organizacyjnej" – art. 3 ust. 1 5

2 Stosowanie kryterium „kierowania" – art. 3 ust. 2 15

3 Przetwarzanie w miejscu, w którym na mocy prawa międzynarodowego publicznego ma zastosowanie prawo państwa członkowskiego 25

4 Przedstawiciele administratorów lub podmiotów przetwarzających niemających jednostki organizacyjnej w Unii 26

Europejska Rada Ochrony Danych

uwzględniając art. 70 ust. 1 lit. e) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE,

PRZYJMUJE NINIEJSZE WYTYCZNE:

WPROWADZENIE

Terytorialny zakres stosowania ogólnego rozporządzenia o ochronie danych[1] (RODO lub rozporządzenie) określono w art. 3 rozporządzenia i stanowi istotny rozwój prawa Unii o ochronie danych w porównaniu z ramami określonymi w dyrektywie 95/46/WE[2]. RODO częściowo potwierdza wybory dokonane przez prawodawcę Unii i Trybunał Sprawiedliwości Unii Europejskiej (TSUE) w kontekście dyrektywy 95/46/WE. Wprowadzono jednak istotne nowe elementy. Co najważniejsze, głównym celem art. 4 dyrektywy było określenie, które prawo krajowe państwa członkowskiego ma zastosowanie, natomiast art. 3 RODO określa zakres terytorialny tekstu mającego bezpośrednie zastosowanie. Ponadto, o ile art. 4 dyrektywy zawierał odniesienie do „wykorzystywania środków" znajdujących się na terytorium Unii jako podstawy objęcia administratorów danych „nieprowadzących działalności gospodarczej na terytorium Wspólnoty" przepisami prawa Unii o ochronie danych, odniesienie takie nie pojawia się w art. 3 RODO.

W art. 3 RODO odzwierciedlono zamiar prawodawcy polegający na zapewnieniu kompleksowej ochrony praw osób, których dane dotyczą w UE oraz ustanowieniu – w kontekście wymogu ochrony danych – równych warunków funkcjonowania dla przedsiębiorstw działających na rynkach UE w kontekście globalnych przepływów danych.

Art. 3 RODO definiuje terytorialny zakres stosowania rozporządzenia na podstawie dwóch głównych kryteriów: kryterium „jednostki organizacyjnej" zgodnie z art. 3 ust. 1 oraz kryterium „kierowania" zgodnie z art. 3 ust. 2. Odpowiednie przepisy RODO będą miały zastosowanie do przetwarzania danych osobowych przez danego administratora danych lub podmiot przetwarzający, jeżeli spełnione jest jedno z tych dwóch kryteriów. Ponadto w art. 3 ust. 3 potwierdzono stosowanie RODO do przetwarzania w miejscu, w którym na mocy prawa międzynarodowego publicznego ma zastosowanie prawo państwa członkowskiego.

Niniejsze wytyczne, dzięki wspólnej interpretacji dokonanej przez organy ochrony danych w UE, mają na celu zapewnienie spójnego stosowania RODO podczas oceny, czy przetwarzanie przez administratora danych lub podmiot przetwarzający jest objęte zakresem stosowania nowych unijnych ram prawnych. W niniejszych wytycznych EROD określa i wyjaśnia kryteria służące określeniu terytorialnego zakresu stosowania RODO. Taka wspólna interpretacja jest również niezbędna dla

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).
[2] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych.

administratorów danych i podmiotów przetwarzających, zarówno w UE jak i poza nią, tak aby mogli oni ocenić, czy powinni przestrzegać przepisów RODO w odniesieniu do danej czynności przetwarzania.

Ponieważ administratorzy danych lub podmioty przetwarzające nieposiadające jednostek organizacyjnych w UE, a zaangażowane w czynności przetwarzania objęte zakresem art. 3 ust. 2, mają obowiązek wyznaczenia przedstawiciela w Unii, niniejsze wytyczne zawierają również wyjaśnienia dotyczące procesu wyznaczania tego przedstawiciela na mocy art. 27 oraz jego zadań i obowiązków.

Europejska Rada Ochrony Danych co do zasady potwierdza, że w przypadku gdy przetwarzanie danych osobowych jest objęte terytorialnym zakresem stosowania RODO, podlega wszystkim przepisom tego rozporządzenia. W niniejszych wytycznych określono różne możliwe scenariusze, w zależności od rodzaju czynności przetwarzania, podmiotu wykonującego takie czynności przetwarzania lub jego lokalizacji, a także szczegółowo określono przepisy mające zastosowanie do każdej sytuacji. W związku z tym istotne jest, aby administratorzy danych i podmioty przetwarzające, zwłaszcza te oferujące towary i usługi na szczeblu międzynarodowym, przeprowadziły staranną ocenę *in concreto* wykonywanych przez nie czynności przetwarzania, aby ustalić, czy związane z tym przetwarzanie danych osobowych jest objęte zakresem stosowania RODO.

Europejska Rada Ochrony Danych podkreśla, że stosowanie art. 3 ma na celu określenie, czy dana czynność przetwarzania, a nie osoba (prawna lub fizyczna), podlega przepisom RODO. W związku z tym niektóre operacje przetwarzania danych osobowych przez administratora danych lub podmiot przetwarzający mogą wchodzić w zakres stosowania rozporządzenia, natomiast inne operacje przetwarzania danych osobowych przez tego samego administratora danych lub podmiot przetwarzający mogą nie wchodzić w zakres stosowania rozporządzenia, w zależności od czynności przetwarzania.

Niniejsze wytyczne, początkowo przyjęte przez EROD 16 listopada, były przedmiotem konsultacji publicznych w okresie od 23 listopada 2018 r. do 18 stycznia 2019 r. i zostały zaktualizowane z uwzględnieniem otrzymanych uwag i informacji zwrotnych.

1 STOSOWANIE KRYTERIUM „JEDNOSTKI ORGANIZACYJNEJ" – ART. 3 UST. 1

Artykuł 3 ust. 1 RODO stanowi, że *rozporządzenie ma zastosowanie do przetwarzania danych osobowych w związku z działalnością prowadzoną przez jednostkę organizacyjną administratora lub podmiotu przetwarzającego w Unii, niezależnie od tego, czy przetwarzanie odbywa się w Unii.*

W art. 3 ust. 1 RODO zawarto odniesienie nie tylko do jednostki organizacyjnej administratora danych, ale również do jednostki organizacyjnej podmiotu przetwarzającego. W rezultacie przetwarzanie danych osobowych przez podmiot przetwarzający może również podlegać prawu Unii, jeżeli podmiot przetwarzający posiada jednostkę organizacyjną na terenie UE.

Art. 3 ust. 1 zapewnia, że RODO stosuje się do przetwarzania dokonywanego przez administratora danych lub podmiot przetwarzający w związku z działalnością prowadzoną przez jednostkę organizacyjną takiego administratora danych lub podmiotu przetwarzającego w Unii, niezależnie od faktycznego miejsca przetwarzania. W związku z tym EROD zaleca stosowanie potrójnego podejścia przy ustalaniu, czy przetwarzanie danych osobowych wchodzi w zakres stosowania RODO zgodnie z art. 3 ust. 1.

W kolejnych działach wyjaśniono stosowanie kryterium jednostki organizacyjnej, po pierwsze biorąc pod uwagę definicję „jednostki organizacyjnej" w UE w rozumieniu unijnego prawa o ochronie danych, po drugie, analizując, co należy rozumieć pod pojęciem „przetwarzania w związku z działalnością jednostki organizacyjnej na terenie Unii", a także potwierdzając, że RODO będzie miało zastosowanie niezależnie od tego, czy przetwarzanie odbywa się w związku z działalnością tej jednostki organizacyjnej na terenie Unii, czy też nie.

a) „Jednostka organizacyjna w Unii"

Przed rozważeniem tego, co należy rozumieć przez „jednostkę organizacyjną w Unii", należy określić, kto jest administratorem danych lub podmiotem przetwarzającym dla danej czynności przetwarzania. Zgodnie z definicją zawartą w art. 4 ust. 7 RODO administrator oznacza „osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych". Podmiot przetwarzający, zgodnie z art. 4 ust. 8 RODO oznacza „osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora". Zgodnie z odpowiednim orzecznictwem TSUE i poprzednią opinią Grupy Roboczej Art. 29[3] ustalenie, czy podmiot jest administratorem lub podmiotem przetwarzającym do celów unijnego prawa o ochronie danych jest kluczowym elementem oceny stosowania RODO do przedmiotowego przetwarzania danych osobowych.

O ile w art. 4 ust. 16 zdefiniowano pojęcie „głównej jednostki organizacyjnej", o tyle w RODO nie zawarto definicji „jednostki organizacyjnej" dla celów art. 3[4]. Motyw 22[5] wyjaśnia jednak, że „[p]ojęcie „jednostka organizacyjna" zakłada skuteczne i faktyczne prowadzenie działalności poprzez stabilne struktury. Forma prawna takich struktur, niezależnie od tego, czy chodzi o oddział czy spółkę zależną posiadającą osobowość prawną, nie jest w tym względzie czynnikiem decydującym".

Brzmienie tego motywu jest identyczne z brzmieniem motywu 19 dyrektywy 95/46/WE, do którego odniesiono się w szeregu orzeczeń TSUE rozszerzających wykładnię pojęcia „jednostka organizacyjna", odchodząc od formalistycznego podejścia, zgodnie z którym przedsiębiorstwa posiadają jednostki organizacyjne wyłącznie w miejscu, w którym posiadają zarejestrowaną siedzibę[6]. Trybunał Sprawiedliwości Unii Europejskiej orzekł bowiem, że pojęcie jednostki organizacyjnej obejmuje wszelką rzeczywistą i faktyczną działalność, choćby nawet drobną, prowadzoną poprzez stabilne rozwiązanie organizacyjne[7]. W celu ustalenia, czy dany podmiot mający siedzibę poza Unią ma jednostkę organizacyjną w państwie członkowskim, należy ocenić stopień stabilności rozwiązania organizacyjnego, jak również faktyczny charakter prowadzenia działalności w tym drugim państwie

[3] Grupa Robocza Art. 29 – Opinia 1/2010 w sprawie pojęć „administrator danych" i „przetwarzający" przyjęta dnia 16 lutego 2010 r. i podlegająca przeglądowi przez EROD.

[4] Definicja „głównej jednostki organizacyjnej" jest istotna głównie do celów określenia kompetencji organów nadzorczych zgodnie z art. 56 RODO. Zobacz Wytyczne Grupy Roboczej Art. 29 dotyczące ustalania wiodącego organu nadzorczego właściwego dla administratora lub podmiotu przetwarzającego (16/EN WP 244 rev.01) zatwierdzone przez EROD.

[5] Motyw 22 RODO: *Przetwarzanie danych osobowych w kontekście działalności prowadzonej przez jednostkę organizacyjną administratora lub podmiotu przetwarzającego w Unii powinno odbywać się zgodnie z niniejszym rozporządzeniem, niezależnie od tego, czy samo przetwarzanie ma miejsce w Unii. Pojęcie »jednostka organizacyjna« zakłada skuteczne i faktyczne prowadzenie działalności poprzez stabilne struktury. Forma prawna takich struktur, niezależnie od tego, czy chodzi o oddział czy spółkę zależną posiadającą osobowość prawną, nie jest w tym względzie czynnikiem decydującym.*

[6] *Zobacz w szczególności: Google Spain SL, Google Inc. przeciwko AEPD, Mario Costeja González (C-131/12), Weltimmo przeciwko NAIH (C-230/14), Verein für Konsumenteninformation przeciwko Amazon EU (C-191/15) i Wirtschaftsakademie Schleswig-Holstein (C-210/16).*

[7] Punkt 31 wyroku w sprawie Weltimmo.

członkowskim, z uwzględnieniem szczególnego charakteru rozpatrywanej działalności gospodarczej oraz świadczenia danych usług. Dotyczy to w szczególności przedsiębiorstw oferujących usługi wyłącznie za pośrednictwem internetu[8].

Próg dla „stabilnych rozwiązań organizacyjnych[9]" może być w rzeczywistości dość niski, jeżeli centrum działalności administratora danych dotyczy świadczenia usług online. W związku z tym w niektórych okolicznościach wystarczającym stabilnym rozwiązaniem organizacyjnym może być obecność w Unii jednego pracownika lub jednego przedstawiciela podmiotu spoza UE (co w rozumieniu art. 3 ust. 1 będzie stanowić „jednostkę organizacyjną"), jeżeli ten pracownik lub przedstawiciel działa z zachowaniem wystarczającego stopnia stabilności. Natomiast w przypadku, gdy pracownik ma siedzibę w UE, ale przetwarzania nie dokonuje się w związku z działalnością pracownika z siedzibą w UE na terenie Unii (tj. przetwarzanie dotyczy działalności administratora poza UE), sama obecność pracownika w UE nie spowoduje, że będzie ono objęte zakresem stosowania RODO. Innymi słowy, obecność pracownika w UE nie jest sama w sobie wystarczająca, aby uruchomić stosowanie RODO, ponieważ przetwarzanie danych, które ma być objęte zakresem stosowania RODO, musi odbywać się również w ramach działalności pracownika z siedzibą w UE.

Fakt, że podmiot spoza UE odpowiedzialny za przetwarzanie danych nie posiada ani filii, ani oddziału w państwie członkowskim, nie wyklucza, że może on tam prowadzić działalność gospodarczą w rozumieniu unijnego prawa o ochronie danych. Chociaż pojęcie jednostki organizacyjnej jest szerokie, nie jest ono pozbawione ograniczeń. Nie można stwierdzić, że podmiot spoza UE posiada jednostkę organizacyjną w Unii na tej tylko podstawie, że witryna internetowa tego przedsiębiorstwa jest tam dostępna[10].

Przykład 1: Przedsiębiorstwo produkujące samochody z siedzibą główną w USA posiada oddział w Brukseli nadzorujący wszystkie jego działania w Europie, w tym marketing i reklamę.

Oddział belgijski można uznać za stabilną strukturę, prowadzącą faktyczną i skuteczną działalność w świetle działalności gospodarczej prowadzonej przez przedsiębiorstwo produkujące samochody. W związku z tym oddział belgijski może być uznany za jednostkę organizacyjną w Unii, w rozumieniu RODO.

Po stwierdzeniu, że administrator danych lub podmiot przetwarzający mają jednostkę organizacyjną w UE, należy przeprowadzić analizę *in concreto* w celu określenia, czy dane przetwarzanie odbywa się w związku z działalnością tej jednostki organizacyjnej, aby ustalić czy zastosowanie ma art. 3 ust. 1. Jeżeli administrator danych lub podmiot przetwarzający mający siedzibę poza Unią prowadzi „faktyczną i rzeczywistą działalność, choćby nawet drobną" poprzez „stabilne rozwiązanie organizacyjne", niezależnie od jego formy (np. jednostka zależna, oddział, biuro...) na terytorium państwa członkowskiego, taki administrator danych lub podmiot przetwarzający posiadają jednostkę organizacyjną w tym państwie członkowskim[11]. Należy zatem rozważyć, czy przetwarzanie danych osobowych odbywa się „w kontekście działalności" takiej jednostki organizacyjnej, jak podkreślono w motywie 22.

[8] Punkt 29 wyroku w sprawie Weltimmo.
[9] Punkt 31 wyroku w sprawie Weltimmo.
[10] TSUE, Verein für Konsumenteninformation przeciwko Amazon EU Sarl, Sprawa C-191/15, 28 lipca 2016 r., punkt 76 (zwana dalej „Verein für Konsumenteninformation").
[11] Zobacz w szczególności pkt 29 wyroku w sprawie Weltimmo, w którym podkreślono elastyczną definicję pojęcia „jednostki organizacyjnej" i wyjaśniono, że „należy ocenić stopień stabilności rozwiązania organizacyjnego, jak również faktyczny charakter prowadzenia działalności w tym drugim państwie członkowskim, z uwzględnieniem szczególnego charakteru rozpatrywanej działalności gospodarczej oraz świadczenia rozpatrywanych usług".

b) Przetwarzanie danych osobowych „w związku z działalnością" prowadzoną przez jednostkę organizacyjną

Art. 3 ust. 1 potwierdza, że nie jest konieczne, aby przetwarzanie było dokonywane „przez" samą konkretną jednostkę organizacyjną w UE; administrator danych lub podmiot przetwarzający będą podlegać obowiązkom wynikającym z RODO za każdym razem, gdy przetwarzanie jest dokonywane „w związku z działalnością" prowadzoną przez daną jednostkę organizacyjną w Unii. Europejska Rada Ochrony Danych zaleca, aby ustalenia, czy przetwarzania dokonuje się w związku z jednostką organizacyjną administratora danych lub podmiotu przetwarzającego w Unii, do celów art. 3 ust. 1 dokonywać dla poszczególnych przypadków w oparciu o analizę *in concreto*. Każdy scenariusz należy oceniać indywidualnie uwzględniając szczególne okoliczności sprawy.

Europejska Rada Ochrony Danych jest zdania, że dla celów art. 3 ust. 1 wyrażenie „przetwarzanie w związku z działalnością prowadzoną przez jednostkę organizacyjną administratora danych lub podmiotu przetwarzającego" należy rozumieć w świetle odpowiedniego orzecznictwa. Z jednej strony, biorąc pod uwagę cel polegający na zapewnieniu skutecznej i pełnej ochrony, w odniesieniu do wyrażenia „w kontekście prowadzenia działalności gospodarczej" nie można przyjmować wykładni zawężającej[12]. Z drugiej strony w odniesieniu do jednostki organizacyjnej w rozumieniu RODO nie można przyjmować wykładni zbyt szerokiej, pozwalającej na stwierdzenie, że samo istnienie jakiejkolwiek jednostki w UE powiązanej w sposób bardzo swobodny z czynnościami przetwarzania podmiotu spoza UE jest wystarczające, aby takie przetwarzanie zostało objęte zakresem stosowania unijnych przepisów o ochronie danych. Niektóre rodzaje działalności handlowej prowadzonej przez podmiot spoza UE w państwie członkowskim mogą być tak dalekie od przetwarzania danych osobowych przez ten podmiot, że istnienie tej działalności handlowej w UE nie spowodowałoby objęcia przetwarzania danych przez podmiot spoza UE zakresem stosowania unijnych przepisów o ochronie danych[13].

Aby ustalić, czy administrator danych lub podmiot przetwarzający przetwarzają dane w związku z ich jednostką organizacyjną w UE, należy uwzględnić dwa następujące czynniki

i) *Relację między administratorem danych lub podmiotem przetwarzającym spoza Unii a ich miejscową jednostką organizacyjną w Unii*

Czynności przetwarzania administratora danych lub podmiotu przetwarzającego z siedzibą poza UE oraz działalność miejscowej jednostki organizacyjnej w państwie członkowskim mogą być nierozerwalnie powiązane, a zatem mogą powodować, iż zastosowanie ma prawo Unii, nawet jeśli jednostka ta w rzeczywistości nie bierze żadnego udziału w samym przetwarzaniu danych[14]. Jeśli z analizy okoliczności w poszczególnych przypadkach wynika, że istnieje nierozerwalny związek między przetwarzaniem danych dokonywanym przez administratora danych lub podmiot przetwarzający spoza UE a działalnością prowadzoną przez jednostkę organizacyjną w UE, prawo Unii będzie miało zastosowanie do tego przetwarzania danych przez podmiot spoza UE, bez względu na to, czy jednostka organizacyjna w UE odgrywa jakąś rolę w tym przetwarzaniu danych[15].

[12] Wyroki w sprawach Weltimmo, pkt 25 i Google Spain, pkt 53.
[13] Grupa Robocza Art. 29, aktualizacja opinii WP 179, Aktualizacja opinii 8/2010 w sprawie prawa właściwego w świetle wyroku Trybunału Sprawiedliwości Unii Europejskiej w sprawie Google Spain, 16 grudnia 2015 r.
[14] TSUE, Google Spain, sprawa C-131/12.
[15] Grupa Robocza Art. 29, aktualizacja opinii WP 179, Aktualizacja opinii 8/2010 w sprawie prawa właściwego w świetle wyroku Trybunału Sprawiedliwości Unii Europejskiej w sprawie Google Spain, 16 grudnia 2015 r.

ii) Generowanie dochodów w Unii

Generowanie dochodów w UE przez miejscową jednostkę organizacyjną – o ile taką działalność można „nierozerwalnie powiązać" z przetwarzaniem danych osobowych odbywającym się poza UE – wystarcza, aby wskazać, że przetwarzanie danych przez administratora danych lub podmiot przetwarzający spoza UE odbywa się w „w związku z działalnością prowadzoną przez jednostkę organizacyjną w UE" oraz aby do tego przetwarzania zastosowanie miało prawo Unii[16].

Europejska Rada Ochrony Danych zaleca, aby organizacje spoza UE przeprowadziły ocenę swoich czynności przetwarzania, określając, po pierwsze, czy dane osobowe są przetwarzane, a po drugie określając potencjalne powiązania między działalnością, w związku z którą dane są przetwarzane, a działalnością organizacji obecnej w Unii. Jeżeli takie powiązanie zostanie stwierdzone, jego charakter będzie miał kluczowe znaczenie dla określenia, czy RODO ma zastosowanie do danego przetwarzania, i należy go ocenić między innymi w odniesieniu do dwóch elementów wskazanych powyżej.

Przykład 2: Przedsiębiorstwo z siedzibą w Chinach obsługuje stronę internetową dotyczącą handlu elektronicznego. Działalność przedsiębiorstwa w zakresie przetwarzania danych osobowych prowadzona jest wyłącznie w Chinach. Chińskie przedsiębiorstwo utworzyło biuro europejskie w Berlinie w celu poszukiwania możliwości handlowych oraz marketingowych i ich wdrażania na rynkach europejskich.

W tym przypadku można uznać, że działalność biura europejskiego w Berlinie jest nierozerwalnie powiązana z przetwarzaniem danych osobowych przez chińską stronę internetową dotyczącą handlu elektronicznego w zakresie, w jakim kampania poszukiwawczo-marketingowa na rynkach europejskich służy przede wszystkim zapewnieniu rentowności usług oferowanych przez stronę internetową dotyczącą handlu elektronicznego. Przetwarzanie danych osobowych przez chińskie przedsiębiorstwo w odniesieniu do sprzedaży w UE jest w istocie nierozerwalnie powiązane z działalnością biura europejskiego w Berlinie odnoszącą się do kampanii poszukiwawczo-marketingowej na rynku europejskim. Przetwarzanie danych osobowych przez chińskie przedsiębiorstwo w związku ze sprzedażą w UE można zatem uznać za dokonywane w związku z działalnością biura europejskiego, jako jednostki organizacyjnej w Unii. Ta działalność przetwarzania prowadzona przez chińskie przedsiębiorstwo będzie zatem podlegać przepisom RODO zgodnie z jego art. 3 ust. 1.

Przykład 3: Sieć hoteli i ośrodków wypoczynkowych w RPA oferuje pakiety poprzez swoją stronę internetową dostępną w języku angielskim, niemieckim, francuskim i hiszpańskim. Przedsiębiorstwo nie posiada żadnego biura, przedstawicielstwa ani stabilnej struktury w UE.

W takim przypadku, wobec braku przedstawicielstwa lub stabilnej struktury tej sieci hoteli i ośrodków wypoczynkowych na terytorium Unii, wydaje się, że żadnego podmiotu powiązanego z tym administratorem danych w RPA nie można uznać za jednostkę organizacją w UE w rozumieniu RODO. Takie przetwarzanie danych nie będzie zatem podlegać przepisom RODO zgodnie z jego art. 3 ust. 1.

[16] Taka sytuacja może mieć na przykład miejsce w przypadku dowolnego obcego operatora, który posiada biuro sprzedaży lub w jakiś inny sposób jest obecny w UE, nawet jeśli to biuro nie odgrywa żadnej roli w rzeczywistym przetwarzaniu danych, zwłaszcza w przypadku, gdy przetwarzanie danych odbywa się w kontekście działalności w zakresie sprzedaży w UE i działalność tej jednostki organizacyjnej skierowana jest do mieszkańców państw członkowskich, w których ta jednostka organizacyjna się znajduje (aktualizacja WP 179).

Należy jednak przeprowadzić analizę *in concreto*, aby określić czy przetwarzanie danych przez tego administratora danych spoza UE może podlegać przepisom RODO zgodnie z art. 3 ust. 2.

c) Zastosowanie RODO do jednostki organizacyjnej administratora danych lub podmiotu przetwarzającego w Unii, niezależnie od tego, czy przetwarzanie danych odbywa się w Unii

Zgodnie z art. 3 ust. 1 przetwarzanie danych osobowych w związku z działalnością prowadzoną przez jednostkę organizacyjną administratora danych lub podmiotu przetwarzającego w Unii skutkuje zastosowaniem RODO i powiązanych zobowiązań w odniesieniu do danego administratora lub podmiotu przetwarzającego.

W treści RODO określono, że rozporządzenie ma zastosowanie do przetwarzania w związku z działalnością prowadzoną przez jednostkę organizacyjną w UE „niezależnie od tego, czy przetwarzanie odbywa się w Unii". To właśnie obecność, w postaci jednostki organizacyjnej, administratora danych lub podmiotu przetwarzającego w UE oraz fakt, że przetwarzanie odbywa się w związku z działalnością takiej jednostki organizacyjnej, skutkuje zastosowaniem RODO do czynności przetwarzania. Miejsce przetwarzania danych nie jest zatem istotne dla ustalenia, czy przetwarzanie, dokonywane w związku z działalnością prowadzoną przez jednostkę organizacyjną w UE, wchodzi w zakres stosowania RODO.

Przykład 4: Francuskie przedsiębiorstwo opracowało aplikację car-sharing skierowaną wyłącznie do klientów w Maroku, Algierii i Tunezji. Usługa jest dostępna jedynie w tych trzech krajach, ale wszystkie czynności przetwarzania danych są prowadzone przez administratora danych we Francji.

Chociaż gromadzenie danych osobowych odbywa się w państwach niebędących członkami UE, dalsze przetwarzanie danych osobowych w tym przypadku odbywa się w związku z działalnością prowadzoną przez jednostkę organizacyjną administratora danych w Unii. W związku z tym, nawet jeśli przetwarzanie dotyczy danych osobowych osób, których dane dotyczą niebędących w UE, przetwarzanie dokonywane przez francuskie przedsiębiorstwo będzie podlegać przepisom RODO, zgodnie z art. 3 ust. 1.

Przykład 5: Firma farmaceutyczna z siedzibą w Sztokholmie zlokalizowała wszystkie swoje czynności przetwarzania danych osobowych w odniesieniu do danych dotyczących badań klinicznych w swoim oddziale w Singapurze.

W takim przypadku przetwarzanie danych odbywa się w Singapurze, jednak odbywa się ono w związku z działalnością firmy farmaceutycznej w Sztokholmie, czyli administratora danych mającego jednostkę organizacyjną w Unii. Przepisy RODO mają zatem zastosowanie do takiego przetwarzania, zgodnie z art. 3 ust. 1.

Przy określaniu terytorialnego zakresu stosowania RODO dla celów art. 3 ust. 1 istotne jest położenie geograficzne miejsca prowadzenia działalności:

- samego administratora danych lub podmiotu przetwarzającego (czy ma swoją siedzibę w Unii, czy poza nią?);
- obecności handlowej administratora danych lub podmiotu przetwarzającego spoza UE (czy posiada on jednostkę organizacyjną w Unii?).

Położenie geograficzne nie ma jednak znaczenia dla celów art. 3 ust. 1 w odniesieniu do miejsca przetwarzania, ani miejsca, w którym znajdują się osoby, których dane dotyczą.

Treść art. 3 ust. 1 nie ogranicza stosowania RODO do przetwarzania danych osobowych osób fizycznych przebywających w Unii. Europejska Rada Ochrony Danych uważa zatem, że przetwarzanie danych osobowych w związku z działalnością prowadzoną przez jednostkę organizacyjną administratora lub podmiotu przetwarzającego w Unii wchodzi w zakres stosowania RODO niezależnie od lokalizacji lub narodowości osoby, której przetwarzane dane dotyczą. Motyw 14 RODO potwierdza tę interpretację i stanowi, że „[o]chrona zapewniana niniejszym rozporządzeniem powinna mieć zastosowanie do osób fizycznych – niezależnie od ich obywatelstwa czy miejsca zamieszkania – w związku z przetwarzaniem ich danych osobowych".

d) Stosowanie kryterium „jednostki organizacyjnej" do administratora danych i podmiotu przetwarzającego

Jeśli chodzi o czynności przetwarzania wchodzące w zakres stosowania art. 3 ust. 1 EROD uważa, że przepisy te mają zastosowanie do administratorów danych i podmiotów przetwarzających, których czynności przetwarzania są dokonywane w związku z działalnością prowadzoną przez ich jednostkę organizacyjną w UE. Uznając, że wymogi dotyczące ustanowienia stosunku między administratorem danych a podmiotem przetwarzającym[17] nie różnią się w zależności od położenia geograficznego jednostki organizacyjnej administratora danych lub podmiotu przetwarzającego, EROD jest zdania, że jeśli chodzi o identyfikację różnych obowiązków wynikających z zastosowania RODO zgodnie z art. 3 ust. 1, przetwarzanie danych przez każdy podmiot należy rozpatrywać oddzielnie.

W RODO przewidziano różne i szczególne przepisy lub obowiązki mające zastosowanie do administratorów danych i podmiotów przetwarzających, w związku z tym, gdyby administrator danych lub podmiot przetwarzający byli objęci zakresem stosowania RODO zgodnie z art. 3 ust. 1, zastosowanie miałyby do nich odpowiednie i odrębne obowiązki z tym związane. W tym kontekście EROD zauważa, że podmiotu przetwarzającego w UE nie powinno się uznawać za jednostkę organizacyjną administratora danych w rozumieniu art. 3 ust. 1 wyłącznie ze względu na jej status podmiotu przetwarzającego dane w imieniu administratora danych.

Istnienie stosunku pomiędzy administratorem danych a podmiotem przetwarzającym nie musi powodować obowiązku stosowania RODO do obu tych podmiotów, jeżeli jeden z nich nie posiada jednostki organizacyjnej w Unii.

Organizacja przetwarzająca dane osobowe w imieniu i na polecenie innej organizacji (przedsiębiorstwa będącego klientem) będzie działać w charakterze podmiotu przetwarzającego dane na rzecz przedsiębiorstwa będącego klientem (administratora danych). Jeżeli podmiot przetwarzający ma jednostkę organizacyjną w Unii, będzie on zobowiązany do przestrzegania obowiązków nałożonych na podmioty przetwarzające na mocy RODO („obowiązki podmiotu przetwarzającego wynikające z RODO"). Jeżeli administrator danych zlecający przetwarzanie podmiotowi przetwarzającemu również znajduje się w Unii, będzie on zobowiązany do przestrzegania obowiązków nałożonych na administratorów danych na mocy RODO („obowiązki administratora danych wynikające z RODO"). Czynność przetwarzania, która – jeśli jest dokonywana przez administratora danych – wchodzi w zakres stosowania RODO na podstawie art. 3 ust. 1, nie będzie wyłączona z zakresu zastosowania tego rozporządzenia tylko dlatego, że administrator danych zleca wykonanie przetwarzania w jego imieniu podmiotowi przetwarzającemu nieposiadającemu jednostki organizacyjnej w Unii.

[17] Zgodnie z art. 28 EROD przypomina, że czynności przetwarzania dokonywane przez podmiot przetwarzający w imieniu administratora danych odbywają się na podstawie umowy lub innego instrumentu prawnego podlegającego prawu Unii lub prawu państwa członkowskiego i wiążącego podmiot przetwarzający względem administratora danych, a ten korzysta wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.

i) Przetwarzanie danych przez administratora danych mającego jednostkę organizacyjną w UE, który zleca czynność podmiotowi przetwarzającemu niemającemu jednostki organizacyjnej w Unii

Jeżeli administrator danych podlegający przepisom RODO postanowi korzystać z usług podmiotu przetwarzającego zlokalizowanego poza Unią do celów danej czynności przetwarzania, administrator danych musi zapewnić, na podstawie umowy lub innego instrumentu prawnego, że podmiot przetwarzający przetwarza dane zgodnie z RODO. Zgodnie z art. 28 ust. 3 przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy lub innego instrumentu prawnego. W związku z tym administrator danych musi zapewnić zawarcie umowy z podmiotem przetwarzającym zawierającą wszystkie wymogi określone w art. 28 ust. 3. Ponadto prawdopodobne jest, że w celu wywiązania się przez administratora ze swoich obowiązków wynikających z art. 28 ust. 1 – korzystania wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą – administrator danych będzie musiał rozważyć nałożenie, w drodze umowy, obowiązków nałożonych przez RODO na podmioty przetwarzające, które mu podlegają. Oznacza to, że administrator danych musiałby dopilnować, aby podmiot przetwarzający, niepodlegający RODO, wypełniał obowiązki określone w umowie lub innym instrumencie prawnym na mocy prawa Unii lub prawa państwa członkowskiego, o których mowa w art. 28 ust. 3.

Podmiot przetwarzający spoza Unii będzie zatem pośrednio podlegał niektórym obowiązkom nałożonym przez administratorów danych podlegających RODO na podstawie ustaleń umownych na mocy art. 28. Ponadto zastosowanie mogą mieć przepisy rozdziału V RODO.

Przykład 6: Fiński instytut badawczy prowadzi prace badawcze dotyczące Lapończyków. Instytut uruchamia projekt, który dotyczy tylko Lapończyków w Rosji. Do realizacji tego projektu instytut wykorzystuje podmiot przetwarzający dane z siedzibą w Kanadzie.

Fiński administrator danych jest zobowiązany do korzystania wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą. Fiński administrator danych musi zawrzeć umowę o przetwarzanie danych z kanadyjskim podmiotem przetwarzającym, a obowiązki podmiotu przetwarzającego zostaną określone w tym instrumencie prawnym.

ii) *Przetwarzanie w związku z działalnością prowadzoną przez jednostkę organizacyjną podmiotu przetwarzającego w Unii*

Chociaż orzecznictwo pozwala na jasne zrozumienie skutków przetwarzania danych dokonywanego w związku z działalnością prowadzoną przez jednostkę organizacyjną administratora danych w UE, skutki przetwarzania danych w związku z działalnością jednostki organizacyjnej podmiotu przetwarzającego w UE są mniej oczywiste.

Europejska Rada Ochrony Danych podkreśla, że przy ustalaniu, czy każda ze stron ma swoją „jednostkę organizacyjną w Unii", ważne jest odrębne rozważenie jednostki organizacyjnej administratora danych i podmiotu przetwarzającego.

Pierwsze pytanie dotyczy tego, czy sam administrator danych posiada jednostkę organizacyjną w Unii i przetwarza dane w związku z działalnością prowadzoną przez tę jednostkę organizacyjną. Zakładając,

że administratora danych nie uznaje się za przetwarzającego w związku ze swoją jednostką organizacyjną w Unii, administrator danych nie będzie podlegał obowiązkom administratora danych wynikającym z RODO na podstawie art. 3 ust. 1 (chociaż może on nadal podlegać przepisom art. 3 ust. 2). O ile nie występują inne czynniki, jednostka organizacyjna podmiotu przetwarzającego w UE nie będzie uważana za jednostkę organizacyjną w odniesieniu do administratora danych.

Pojawia się zatem odrębne pytanie, czy podmiot przetwarzający przetwarza dane w związku z działalnością prowadzoną przez jego jednostkę organizacyjną w Unii. Jeżeli tak, podmiot przetwarzający będzie podlegał obowiązkom podmiotu przetwarzającego wynikającym z RODO na mocy art. 3 ust. 1. Nie powoduje to jednak, że administrator danych spoza UE podlega obowiązkom administratora danych wynikającym z RODO. Oznacza to, że administrator danych „spoza UE" (jak opisano powyżej) nie będzie podlegał przepisom RODO tylko dlatego, że zdecyduje się skorzystać z usług podmiotu przetwarzającego w Unii.

Zlecenie przetwarzania danych podmiotowi przetwarzającemu w Unii nie spowoduje, że administrator danych będzie podlegać przepisom RODO i dokonywać przetwarzania danych „w związku z działalnością prowadzoną przez podmiot przetwarzający w Unii". Przetwarzanie odbywa się w związku z działalnością administratora danych; podmiot przetwarzający świadczy jedynie usługę przetwarzania[18], która nie jest „nierozerwalnie powiązana" z działalnością administratora danych. Jak stwierdzono powyżej, w przypadku podmiotu przetwarzającego mającego jednostkę organizacyjną w Unii i przetwarzającego dane w imieniu administratora danych spoza Unii i niepodlegającego przepisom RODO zgodnie z art. 3 ust. 2, EROD uważa że czynności przetwarzania administratora danych nie zostałyby uznane za wchodzące w terytorialny zakres stosowania RODO tylko dlatego, że przetwarzania w imieniu administratora danych dokonuje podmiot przetwarzający mający jednostkę organizacyjną w Unii. Mimo, że administrator danych nie ma jednostki organizacyjnej w Unii i nie podlega przepisom RODO zgodnie z art. 3 ust. 2, podmiot przetwarzający, mający jednostkę organizacyjną w Unii, będzie jednak podlegał odpowiednim przepisom RODO zgodnie z art. 3 ust. 1.

Przykład 7: Meksykańskie przedsiębiorstwo prowadzące działalność w zakresie handlu detalicznego zawiera umowę z podmiotem przetwarzającym mającym jednostkę organizacyjną w Hiszpanii, dotyczącą przetwarzania danych osobowych klientów meksykańskiego przedsiębiorstwa. Meksykańskie przedsiębiorstwo oferuje swoje usługi wyłącznie na rynku meksykańskim i do tego rynku usługi są skierowane, a przetwarzanie dotyczy wyłącznie osób, których dane dotyczą, znajdujących się poza terytorium Unii.

W takim przypadku meksykańskie przedsiębiorstwo nie kieruje swoich towarów ani usług do osób znajdujących się na terytorium Unii, ani nie monitoruje zachowania osoby na terytorium Unii. Przetwarzanie danych przez administratora danych mającego siedzibę poza Unią nie podlega zatem przepisom RODO zgodnie z art. 3 ust. 2.

Przepisów RODO nie stosuje się do administratora danych na podstawie art. 3 ust. 1, ponieważ nie przetwarza on danych osobowych w związku z działalnością prowadzoną przez jednostkę organizacyjną w Unii. Podmiot przetwarzający posiada jednostkę organizacyjną w Hiszpanii, a zatem przetwarzanie przez niego danych wchodzi w zakres stosowania RODO na podstawie art. 3 ust. 1. Podmiot przetwarzający będzie zobowiązany do przestrzegania obowiązków podmiotu przetwarzającego nałożonych na mocy rozporządzenia w odniesieniu do każdej czynności przetwarzania dokonywanej w związku z jego działalnością.

[18] Oferowania usługi przetwarzania w tym kontekście nie można również uznać za oferowanie usługi osobom, których dane dotyczą, w Unii.

Jeżeli podmiot przetwarzający posiadający jednostkę organizacyjną w Unii dokonuje przetwarzania w imieniu administratora danych niemającego jednostki organizacyjnej w Unii do celów czynności przetwarzania i nieobjętego terytorialnym zakresem stosowania RODO zgodnie z art. 3 ust. 2, taki podmiot przetwarzający będzie podlegał następującym stosownym przepisom RODO mającym bezpośrednie zastosowanie do podmiotów przetwarzających dane:

- Obowiązki nałożone na podmioty przetwarzających na mocy art. 28 ust. 2, 3, 4, 5, i 6, dotyczące obowiązku zawarcia umowy powierzenia przetwarzania danych, z wyjątkiem obowiązków dotyczących udzielenia pomocy administratorowi danych w wywiązaniu się z jego obowiązków (administratora danych) wynikających z RODO.
- Podmiot przetwarzający oraz każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego i mająca dostęp do danych osobowych przetwarzają je wyłącznie na polecenie administratora, chyba że wymaga tego prawo Unii lub prawo państwa członkowskiego, zgodnie z art. 29 i art. 32 ust. 4.
- W stosownych przypadkach podmiot przetwarzający prowadzi rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora danych, zgodnie z art. 30 ust. 2.
- W stosownych przypadkach podmiot przetwarzający, na żądanie, współpracuje z organem nadzorczym w ramach wykonywania przez niego swoich zadań, zgodnie z art. 31.
- Podmiot przetwarzający wdraża odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku, zgodnie z art. 32.
- Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi danych, zgodnie z art. 33.
- W stosownych przypadkach podmiot przetwarzający wyznacza inspektora ochrony danych, zgodnie z art. 37 i 38.
- Przepisy dotyczące przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych, zgodnie z rozdziałem V.

Ponadto ponieważ takie przetwarzanie odbywałoby się związku z działalnością prowadzoną przez jednostkę organizacyjną podmiotu przetwarzającego w Unii, EROD przypomina, że podmiot przetwarzający będzie musiał zapewnić zgodność przetwarzania z pozostałymi zobowiązaniami wynikających z prawa Unii lub prawa krajowego. Artykuł 28 ust. 3 stanowi również, że „podmiot przetwarzający niezwłocznie informuje administratora, jeżeli jego zdaniem wydane mu polecenie stanowi naruszenie niniejszego rozporządzenia lub innych przepisów Unii lub państwa członkowskiego o ochronie danych".

Zgodnie ze stanowiskiem zajętym wcześniej przez Grupę Roboczą Art. 29, EROD jest zdania, że terytorium Unii nie może być wykorzystywane jako „bezpieczna przystań" dla przechowywania danych, na przykład gdy działanie polegające na przetwarzaniu wiąże się z niedopuszczalnymi z etycznego punktu widzenia treściami[19], oraz że podmiot przetwarzający mający jednostkę organizacyjną w Unii musi przestrzegać pewnych zobowiązań prawnych wykraczających poza zakres stosowania unijnego prawa o ochronie danych, w szczególności przepisów unijnych i krajowych dotyczących porządku publicznego, niezależnie od miejsca, w którym znajduje się administrator danych. W tym kontekście uwzględniono również fakt, że poprzez wdrożenie prawa Unii przepisy wynikające z RODO i powiązane przepisy krajowe podlegają Karcie praw podstawowych Unii Europejskiej[20]. Nie wiąże się to jednak z nałożeniem dodatkowych obowiązków na administratorów

[19] Grupa Robocza Art. 29 – Opinia 1/2010 w sprawie pojęć „administrator danych" i „przetwarzający" przyjęta dnia 16 lutego 2010 r. i podlegająca przeglądowi przez EROD.
[20] Karta praw podstawowych Unii Europejskiej, 2012/C 326/02.

danych spoza Unii w odniesieniu do przetwarzania, które nie wchodzi w zakres terytorialny stosowania RODO.

2 STOSOWANIE KRYTERIUM „KIEROWANIA" – ART. 3 UST. 2

Brak jednostki organizacyjnej w Unii niekoniecznie oznacza, że czynności przetwarzania dokonywane przez administratora danych lub podmiot przetwarzający z siedzibą w państwie trzecim będą wyłączone z zakresu stosowania RODO, ponieważ w art. 3 ust. 2 określono okoliczności, w których przepisy RODO mają zastosowanie do administratora danych lub podmiotu przetwarzającego niemającego jednostki organizacyjnej w Unii w zależności od ich działalności związanej z przetwarzaniem.

W tym kontekście EROD potwierdza, że w przypadku braku jednostki organizacyjnej w Unii administrator danych lub podmiot przetwarzający nie mogą korzystać z mechanizmu kompleksowej współpracy, o którym mowa w art. 56 RODO. Mechanizm współpracy i spójności przewidziany w RODO ma zastosowanie wyłącznie do administratorów danych i podmiotów przetwarzających, posiadających jednostkę organizacyjną lub jednostki organizacyjne w Unii Europejskiej[21].

Chociaż celem niniejszych wytycznych jest wyjaśnienie terytorialnego zakresu stosowania RODO, EROD pragnie także podkreślić, że administratorzy danych i podmioty przetwarzające będą również musiały uwzględniać inne mające zastosowanie teksty, takie jak na przykład przepisy sektorowe Unii lub państw członkowskich oraz przepisy krajowe. Niektóre przepisy RODO faktycznie umożliwiają państwom członkowskim wprowadzenie dodatkowych warunków i określenie szczególnych ram ochrony danych na szczeblu krajowym w pewnych obszarach lub w odniesieniu do szczególnych sytuacji w zakresie przetwarzania. Administratorzy danych i podmioty przetwarzające powinny zatem zadbać o to, by być świadomi istnienia takich dodatkowych warunków i ram, które mogą się różnić w poszczególnych państwach członkowskich, oraz aby postępować zgodnie z tymi dodatkowymi warunkami i ramami. Takie różnice w przepisach dotyczących ochrony danych, mające zastosowanie w każdym państwie członkowskim, są szczególnie istotne w odniesieniu do przepisów art. 8 (zgodnie z którym wiek, w którym dzieci mogą udzielić ważnej zgody dotyczącej przetwarzania ich danych w związku z usługami społeczeństwa informacyjnego, może się różnić w od 13 do 16), art. 9 (w odniesieniu do przetwarzania szczególnych kategorii danych), art. 23 (ograniczenia) lub przepisów zawartych w rozdziale IX RODO (wolność wypowiedzi i informacji; publiczny dostęp do dokumentów urzędowych; krajowy numer identyfikacyjny; przetwarzanie w kontekście zatrudnienia; przetwarzanie do celów archiwalnych w interesie publicznym; przetwarzanie do celów badań naukowych lub historycznych lub do celów statystycznych; zachowanie tajemnicy; kościoły i związki wyznaniowe).

Zgodnie z art. 3 ust. 2 RODO „niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych osób, których dane dotyczą, przebywających w Unii przez administratora lub podmiot przetwarzający niemających jednostek organizacyjnych w Unii, jeżeli czynności przetwarzania wiążą się z: *oferowaniem towarów lub usług takim osobom, których dane dotyczą, w Unii – niezależnie od tego, czy wymaga się od tych osób zapłaty; lub b) monitorowaniem ich zachowania, o ile do zachowania tego dochodzi w Unii.*"

Stosowanie „kryterium kierowania" w odniesieniu do osób, których dane dotyczą przebywających w Unii, zgodnie z art. 3 ust. 2, może wynikać z czynności przetwarzania prowadzonych przez

[21] Grupa Robocza Art. 29, WP244 rev.1, 13 grudnia 2016 r., Wytyczne dotyczące ustalania wiodącego organu nadzorczego właściwego dla administratora lub podmiotu przetwarzającego zatwierdzone przez EROD.

administratora danych lub podmiot przetwarzający niemający jednostki organizacyjnej w Unii, które odnoszą się do dwóch odrębnych i alternatywnych rodzajów czynności, pod warunkiem że te czynności przetwarzania odnoszą się do osób, których dane dotyczą, przebywających w Unii. Kryterium kierowania, oprócz tego, że ma zastosowanie wyłącznie do przetwarzania danych przez administratora danych lub podmiot przetwarzający niemający jednostki organizacyjnej w Unii, w dużej mierze koncentruje się na tym, z czym „czynności przetwarzania" są „związane", co należy rozpatrywać w poszczególnych przypadkach.

Europejska Rada Ochrony Danych podkreśla, że administrator danych lub podmiot przetwarzający mogą podlegać przepisom RODO w odniesieniu do niektórych rodzajów czynności przetwarzania, przy czym nie muszą podlegać tym przepisom w odniesieniu do innych czynności przetwarzania. Elementem decydującym o terytorialnym stosowaniu RODO zgodnie z art. 3 ust. 2, jest rozpatrzenie przedmiotowych czynności przetwarzania.

Oceniając warunki stosowania kryterium „kierowania" EROD zaleca zatem dwutorowe podejście w celu ustalenia, po pierwsze, że przetwarzanie dotyczy danych osobowych osób, których dane dotyczą, przebywających w Unii, a po drugie, czy przetwarzanie dotyczy oferowania towarów lub usług lub monitorowania zachowania osób, których dane dotyczą, w Unii.

a) Osoby, których dane dotyczą przebywające w Unii

Brzmienie art. 3 ust 2 odnosi się do „danych osobowych osób, których dane dotyczą, przebywających w Unii". Stosowanie kryterium „kierowania" nie jest zatem ograniczone przez obywatelstwo, miejsce pobytu ani inny rodzaj statusu prawnego osoby, której dane dotyczą, której dane osobowe są przetwarzane. Motyw 14 RODO potwierdza tę interpretację i stanowi, że „[o]chrona zapewniana niniejszym rozporządzeniem powinna mieć zastosowanie do osób fizycznych – niezależnie od ich obywatelstwa czy miejsca zamieszkania – w związku z przetwarzaniem ich danych osobowych".

Ten przepis RODO stanowi odzwierciedlenie prawa pierwotnego UE, które przewiduje również szeroki zakres ochrony danych osobowych, nie tylko obywateli UE, wynikający z art. 8 Karty praw podstawowych, który stanowi, że prawo do ochrony danych osobowych nie jest ograniczone, ale dotyczy „wszystkich"[22].

Jakkolwiek przebywanie osoby, której dane dotyczą, na terytorium Unii jest czynnikiem decydującym dla zastosowania kryterium „kierowania" zgodnie z art. 3 ust. 2, EROD uważa, że obywatelstwo lub status prawny osoby, której dane dotyczą, przebywającej na terytorium Unii, nie może ograniczać terytorialnego zakresu stosowania rozporządzenia.

Wymóg, aby osoba, której dane dotyczą, przebywała w Unii, należy ocenić w momencie, w którym ma miejsce odpowiednie działanie inicjujące, tj. w momencie oferowania towarów lub usług, lub w momencie, w którym monitorowane jest zachowanie, niezależnie od czasu trwania oferty lub monitorowania.

EROD uważa jednak, że w odniesieniu do czynności przetwarzania związanych z ofertą usług, przepis ten dotyczy czynności, które w sposób zamierzony, a nie w sposób niezamierzony lub przypadkowy, są skierowane do osób fizycznych w UE. W związku z tym, jeżeli przetwarzanie dotyczy usługi, która jest oferowana wyłącznie osobom fizycznym spoza UE, ale nie zostanie wycofana, w momencie gdy takie osoby wjeżdżają do UE, odnośne przetwarzanie nie będzie podlegało przepisom RODO. W tym

[22] Karta praw podstawowych Unii Europejskiej, art. 8 ust. 1, „Każdy ma prawo do ochrony danych osobowych, które go dotyczą".

przypadku przetwarzanie nie jest związane z celowym zwracaniem się do osób fizycznych w UE, ale do osób fizycznych spoza UE, które będzie kontynuowane niezależnie od tego, czy takie osoby przebywają poza UE czy też odwiedzają Unię.

Przykład 8: Australijskie przedsiębiorstwo oferuje usługi mobilnego serwisu informacyjnego i treści wideo oparte na preferencjach i interesach użytkowników. Użytkownicy mogą otrzymywać aktualne treści codziennie lub co tydzień. Usługa jest oferowana wyłącznie użytkownikom znajdującym się w Australii, którzy podczas dokonywania subskrypcji muszą dostarczyć australijski numer telefonu.

Abonent z Australii podróżuje do Niemiec podczas wakacji i nadal korzysta z usługi.

Pomimo iż abonent z Australii będzie korzystał z tej usługi podczas pobytu w UE, usługa ta nie jest skierowana do osób fizycznych w Unii, lecz wyłącznie do osób fizycznych w Australii, a zatem przetwarzanie danych osobowych przez australijskie przedsiębiorstwo nie wchodzi w zakres stosowania RODO.

Przykład 9: Przedsiębiorstwo typu start-up z siedzibą w USA nieobecne i niemające żadnej jednostki organizacyjnej w UE oferuje aplikację mapową dla turystów. Aplikacja przetwarza dane osobowe dotyczące lokalizacji klientów z niej korzystających (osób, których dane dotyczą), po rozpoczęciu korzystania z aplikacji w odwiedzanym mieście, w celu zaoferowania ukierunkowanej reklamy miejsc wartych odwiedzenia, restauracji, barów i hoteli. Aplikacja jest dostępna dla turystów podczas ich wizyty w Nowym Jorku, San Francisco, Toronto, Paryżu i Rzymie.

Amerykańskie przedsiębiorstwo typu start-up, za pomocą swojej aplikacji mapowej, zwraca się w szczególności do osób fizycznych w Unii (mianowicie w Paryżu i Rzymie) poprzez oferowanie im swoich usług, gdy przebywają one w Unii. Przetwarzanie danych osobowych osób, których dane dotyczą, przebywających w Unii w związku z oferowaniem usługi wchodzi w zakres stosowania RODO zgodnie z art. 3 ust. 2 lit. a). Ponadto poprzez przetwarzanie danych dotyczących lokalizacji osoby, której dane dotyczą, w celu oferowania ukierunkowanej reklamy na podstawie ich lokalizacji, czynności przetwarzania dotyczą również monitorowania zachowania osób fizycznych w Unii. Przetwarzanie przez amerykańskie przedsiębiorstwo typu start-up wchodzi zatem w zakres stosowania RODO zgodnie z art. 3 ust. 2 lit. b).

Europejska Rada Ochrony Danych pragnie również podkreślić, że samo przetwarzanie danych osobowych osoby fizycznej w Unii nie jest wystarczające, aby spowodować zastosowanie RODO do czynności przetwarzania administratora danych lub podmiotu przetwarzającego niemających jednostki organizacyjnej w Unii. Element „kierowania" do osób w UE, poprzez oferowanie towarów lub usług lub monitorowanie ich zachowania (jak wyjaśniono poniżej), musi być zawsze obecny.

Przykład 10: Obywatel Stanów Zjednoczonych podróżuje po Europie w czasie swoich wakacji. Podczas pobytu w Europie pobiera i korzysta z aplikacji informacyjnej oferowanej przez amerykańskie przedsiębiorstwo. Aplikacja jest skierowana wyłącznie na rynek Stanów Zjednoczonych, co wyraźne wynika z warunków korzystania z aplikacji i informacji na temat wskazania dolara amerykańskiego jako jedynej dostępnej waluty płatności. Gromadzenie danych osobowych amerykańskiego turysty za pośrednictwem aplikacji przez amerykańskie przedsiębiorstwo nie jest objęte RODO.

Ponadto należy zauważyć, że przetwarzanie danych osobowych obywateli lub rezydentów UE, które odbywa się w państwie trzecim nie powoduje zastosowania RODO, o ile przetwarzanie nie jest

związane z konkretną ofertą skierowaną do osób fizycznych w UE lub monitorowaniem ich zachowania w Unii.

Przykład 11: Bank w Tajwanie ma klientów mieszkających w Tajwanie, ale posiadających obywatelstwo niemieckie. Bank prowadzi działalność wyłącznie w Tajwanie; jego działalność nie jest skierowana na rynek UE. Przekazywanie danych osobowych niemieckich klientów przez bank nie podlega przepisom RODO.

Przykład 12: Kanadyjski organ imigracyjny przetwarza dane osobowe obywateli UE wjeżdżających na terytorium Kanady w celu rozpatrzenia ich wniosku wizowego. Przetwarzanie to nie podlega RODO.

b) Oferowanie towarów lub usług osobom, których dane dotyczą, niezależnie od tego, czy wymaga się od tych osób zapłaty

Pierwszym działaniem powodującym zastosowanie art. 3 ust. 2 jest „oferowanie towarów lub usług", którą to koncepcję uwzględniono w szerszym zakresie w prawie Unii i orzecznictwie, które należy wziąć pod uwagę przy stosowaniu kryterium „kierowania". Oferowanie usług obejmuje również oferowanie usług społeczeństwa informacyjnego określonych w art. 1 ust. 1 lit. b) dyrektywy (UE) 2015/1535[23] jako „każdą usługę społeczeństwa informacyjnego, to znaczy każdą usługę normalnie świadczoną za wynagrodzeniem, na odległość, drogą elektroniczną i na indywidualne żądanie odbiorcy usług."

Zgodnie z art. 3 ust. 2 kryterium „kierowania" dotyczące oferowania towarów lub usług ma zastosowanie niezależnie od tego, czy od osoby, której dane dotyczą, wymaga się zapłaty. To, czy działalność administratora danych lub podmiotu przetwarzającego niemającego jednostki organizacyjnej w Unii należy uznać za ofertę towaru lub usługi, nie zależy zatem od tego, czy w zamian za dostarczone towary lub usługi dokonuje się zapłaty[24].

Przykład 13: Przedsiębiorstwo z USA niemające jednostki organizacyjnej w UE przetwarza dane osobowe swoich pracowników, którzy przebywali w tymczasowej podróży służbowej we Francji, w Belgii i Holandii dla celów związanych z zasobami kadrowymi, zwłaszcza w celu dokonania zwrotu kosztów zakwaterowania i wypłaty dziennej diety, które różnią się w zależności od państwa, w którym przebywają.

W tej sytuacji, o ile czynności przetwarzania są ściśle związane z osobami na terytorium Unii (tj. pracownikami tymczasowo przebywającymi we Francji, w Belgii i Holandii) nie dotyczą one oferty usługi skierowanej do tych osób, a raczej stanowią część przetwarzania niezbędnego do wypełnienia przez pracodawcę zobowiązań umownych i obowiązków kadrowych związanych z zatrudnieniem danej osoby. Czynność przetwarzania nie ma związku z oferowaniem usługi, nie podlega zatem przepisom RODO zgodnie z art. 3 ust. 2 lit. a).

Innym kluczowym elementem, który należy ocenić przy ustalaniu, czy spełnione jest kryterium „kierowania" zgodnie z art. 3 ust. 2 lit. a), jest to, czy oferta towarów lub usług jest skierowana do osoby w Unii, innymi słowy, czy zachowanie administratora danych, który określa sposoby i cele przetwarzania, wskazuje na zamiar oferowania towarów lub usług osobie, której dane dotyczą, zlokalizowanej w Unii. W motywie 23 RODO wyjaśniono, że „aby stwierdzić, czy administrator lub

[23] Dyrektywa (UE) 2015/1535 Parlamentu Europejskiego i Rady z dnia 9 września 2015 r. ustanawiająca procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego.

[24] Zobacz w szczególności, TSUE, C-352/85, Bond van Adverteerders i inni przeciwko Państwu Holenderskiemu, wyrok z dnia 26 kwietnia 1988 r., punkt 16 oraz TSUE, C-109/92, Wirth [1993] Racc. I-6447, punkt 15.

podmiot przetwarzający oferują towary lub usługi znajdującym się w Unii osobom, których dane dotyczą, należy ustalić, czy jest oczywiste, że administrator lub podmiot przetwarzający planują oferować usługi osobom, których dane dotyczą, w co najmniej jednym państwie członkowskim Unii".

W motywie wyjaśniono ponadto, że „o ile do ustalenia takiego zamiaru nie wystarczy sama dostępność w Unii strony internetowej administratora, podmiotu przetwarzającego, pośrednika, adresu poczty elektronicznej lub innych danych kontaktowych ani posługiwanie się językiem powszechnie stosowanym w państwie trzecim, w którym jednostkę organizacyjną ma administrator, o tyle potwierdzeniem oczywistości faktu, że administrator planuje oferować w Unii towary lub usługi osobom, których dane dotyczą, mogą być czynniki takie, jak posługiwanie się językiem lub walutą powszechnie stosowanymi w co najmniej jednym państwie członkowskim oraz możliwość zamówienia towarów i usług w tym języku lub wzmianka o klientach lub użytkownikach znajdujących się w Unii".

Elementy wymienione w motywie 23 są zgodne z orzecznictwem Trybunału Sprawiedliwości Unii Europejskiej na podstawie rozporządzenia Rady (WE) 44/2001[25] w sprawie jurysdykcji i uznawania orzeczeń sądowych oraz ich wykonywania w sprawach cywilnych i handlowych, w szczególności jego art. 15 ust. 1 lit. c). W sprawach połączonych Peter Pammer przeciwko Reederei Karl Schlüter GmbH & Co iHotel Alpenhof GesmbH przeciwko Oliverowi Hellerowi (sprawy połączone C-585/08 i C-144/09), zwrócono się do Trybunału o wyjaśnienie, co oznacza „kierowanie działalności" w rozumieniu art. 15 ust. 1 lit. c) rozporządzenia 44/2001 (Bruksela I). Trybunał Sprawiedliwości Unii Europejskiej orzekł, że w celu ustalenia, czy przedsiębiorca kieruje działalność do państwa członkowskiego, na terytorium którego konsument ma miejsce zamieszkania w rozumieniu art. 15 ust. 1 lit. c) rozporządzenia Bruksela I, przedsiębiorca musi wyrazić swoją wolę ustanowienia relacji gospodarczych z konsumentem. W tym kontekście TSUE uznał dowody mogące wykazać, że przedsiębiorca zamierza prowadzić interesy z konsumentami mającymi miejsce zamieszkania w państwie członkowskim.

O ile pojęcie „kierowania działalności" różni się od pojęcia „oferowania towarów lub usług" EROD uważa, że orzecznictwo w sprawach połączonych Peter Pammer przeciwko Reederei Karl Schlüter GmbH & Co iHotel Alpenhof GesmbH przeciwko Oliverowi Hellerowi (sprawy połączone C-585/08 i C-144/09)[26] może być pomocne przy rozważaniu, czy towary lub usługi są oferowane osobom, których dane dotyczą, znajdującym się w Unii. Biorąc pod uwagę szczególne okoliczności sprawy, należy uwzględnić między innymi następujące czynniki lub ich połączenie:

- Unia Europejska lub co najmniej jedno państwo członkowskie są wskazane z nazwy w odniesieniu do oferowanych towarów lub usług;
- Administrator danych lub podmiot przetwarzający płacą operatorowi wyszukiwarki internetowej za usługę odsyłania w internecie w celu ułatwienia konsumentom dostępu do swojej strony w Unii; albo administrator lub podmiot przetwarzający rozpoczęli kampanie marketingowe i reklamowe skierowane do odbiorców w UE.
- Międzynarodowy charakter działalności, np. niektóre rodzaje działalności turystycznej;
- Podanie adresów lub numerów telefonicznych dostępnych z państwa UE.

[25] Rozporządzenie Rady (WE) nr 44/2001 z dnia 22 grudnia 2000 r. w sprawie jurysdykcji i uznawania orzeczeń sądowych oraz ich wykonywania w sprawach cywilnych i handlowych.

[26] Jest to tym bardziej istotne, że zgodnie z art. 6 rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 593/2008 z dnia 17 czerwca 2008 r. w sprawie prawa właściwego dla zobowiązań umownych (Rzym I), w przypadku braku wyboru prawa, kryterium „kierowania działalności" do państwa, w którym konsument ma miejsce zwykłego pobytu, uwzględnia się w celu wskazania prawa miejsca zwykłego pobytu konsumenta jako prawa właściwego dla umowy.

- Używanie domeny najwyższego poziomu innej niż domena państwa trzeciego, w którym administrator danych lub podmiot przetwarzający mają siedzibę, np. „.de", czy używanie neutralnych domen pierwszego poziomu takich jak „.eu";
- Opis tras z jednego lub kilku państw członkowskich UE do miejsca świadczenia usługi;
- Wzmianka o międzynarodowej klienteli złożonej z klientów zamieszkałych w różnych państwach członkowskich UE, w szczególności poprzez przedstawienie ich opinii;
- Używanie innego języka lub innej waluty niż używane zwyczajowo w państwie trzecim przedsiębiorcy, w szczególności języka lub waluty jednego lub kilku państw członkowskich UE;
- Administrator danych oferuje dostawę towarów w państwach członkowskich UE.

Jak już wspomniano, niektóre z wyżej wymienionych elementów analizowane pojedynczo mogą nie stanowić wyraźnej wskazówki, co do zamiaru administratora danych oferowania towarów lub usług osobom, których dane dotyczą, przebywającym w Unii, powinno się je jednak uwzględnić w analizie *in concreto* w celu ustalenia, czy połączenie czynników związanych z działalnością handlową administratora danych można łącznie uznać za oferowanie towarów lub usług skierowane do osób, których dane dotyczą, przebywających w Unii.

Należy jednak przypomnieć, że w motywie 23 potwierdzono, że do ustalenia czy administrator danych lub podmiot przetwarzający mają zamiar oferować towary lub usługi osobom, których dane dotyczą przebywającym w Unii, nie wystarczy sama dostępność w Unii strony internetowej administratora danych, podmiotu przetwarzającego, pośrednika, adresu poczty elektronicznej lub adresu geograficznego, bądź numeru telefonu z międzynarodowym numerem kierunkowym. W tym kontekście EROD przypomina, że jeżeli towary lub usługi dostarcza się osobie na terytorium Unii przypadkowo lub incydentalnie, związane z tym przetwarzanie danych osobowych nie wchodzi w terytorialny zakres stosowania RODO.

Przykład 14: Strona internetowa, zlokalizowana i zarządzana w Turcji, oferuje usługi tworzenia, edycji, drukowania i wysyłki spersonalizowanych albumów ze zdjęciami rodzinnymi. Strona internetowa jest dostępna w języku angielskim, francuskim, niderlandzkim i niemieckim, a płatności można dokonywać w euro. Na stronie wskazano, że albumy fotograficzne dostarcza się wyłącznie pocztą we Francji, krajach Beneluksu i w Niemczech.

W tym przypadku jasne jest, że tworzenie, edytowanie i drukowanie spersonalizowanych albumów ze zdjęciami rodzinnymi stanowi usługę w rozumieniu prawa Unii. Fakt, że strona internetowa jest dostępna w czterech językach UE oraz że albumy fotograficzne dostarcza się pocztą w sześciu państwach członkowskich UE, świadczy o tym, że w ramach tureckiej strony internetowej planuje się oferowanie usług osobom fizycznym w Unii.

W związku z tym oczywiste jest, że przetwarzanie dokonywane przez turecką stronę internetową jako administratora danych odnosi się do oferowania usługi osobom, których dane dotyczą, przebywającym w Unii i w związku z tym podlega obowiązkom i przepisom RODO, zgodnie z art. 3 ust. 2 lit. a) RODO.

Zgodnie z art. 27 administrator danych będzie musiał wyznaczyć przedstawiciela w Unii.

Przykład 15: Prywatne przedsiębiorstwo z siedzibą w Monako przetwarza dane osobowe swoich pracowników do celów wypłaty wynagrodzenia. Pracownicy przedsiębiorstwa to w dużej mierze mieszkańcy Francji i Włoch.
W tym przypadku, jakkolwiek przetwarzanie dokonywane przez przedsiębiorstwo odnosi się do osób, których dane dotyczą, we Francji i we Włoszech, nie odbywa się ono w kontekście oferowania towarów lub usług. W istocie zarządzanie zasobami kadrowymi, w tym wypłata wynagrodzenia przez

przedsiębiorstwo z państwa trzeciego, nie może być uznane za oferowanie usługi w rozumieniu art. 3 ust. 2 lit. a); przedmiotowe przetwarzanie nie odnosi się do oferowania towarów lub usług osobom, których dane dotyczą, przebywającym w Unii (ani do monitorowania zachowania), a co za tym idzie, nie podlega przepisom RODO zgodnie z art. 3.

Ocena ta pozostaje bez uszczerbku dla prawa właściwego danego państwa trzeciego.

Przykład 16: Szwajcarski uniwersytet w Zurychu rozpoczyna rekrutację na studia magisterskie udostępniając platformę internetową, na którą kandydaci mogą przesłać swoje CV i list motywacyjny wraz z ich danymi kontaktowymi. Rekrutacja jest otwarta dla każdego studenta ze znajomością języka niemieckiego i angielskiego na wystarczającym poziomie oraz posiadającego dyplom licencjata. Uniwersytet nie reklamuje się szczególnie wśród studentów na uniwersytetach europejskich i przyjmuje płatności wyłącznie w walucie krajowej.

Ponieważ w procedurze aplikowania i wyboru studentów na te studia magisterskie nie przewidziano rozróżnienia ani specyfikacji dla studentów z Unii, nie można stwierdzić, że uniwersytet szwajcarski ma zamiar dotrzeć do studentów z określonych państw członkowskich UE. Wystarczająca znajomość języka niemieckiego i angielskiego jest ogólnym wymogiem mającym zastosowanie do każdego kandydata, niezależnie od tego, czy jest on rezydentem Szwajcarii, osobą z Unii, czy też studentem z państwa trzeciego. Bez uwzględnienia innych czynników wskazujących na ukierunkowanie się na studentów w państwach członkowskich UE, nie można stwierdzić, że przedmiotowe przetwarzanie odnosi się do oferowania usług edukacyjnych osobom, których dane dotyczą, przebywającym w Unii, w związku z czym takie przetwarzanie nie będzie podlegało przepisom RODO.

Szwajcarski uniwersytet oferuje również kursy letnie w ramach stosunków międzynarodowych i kieruje swoją ofertę w szczególności do uniwersytetów niemieckich i austriackich, aby maksymalnie zwiększyć frekwencję. W takim przypadku szwajcarski uniwersytet wyraźnie oferuje takie usługi osobom, których dane dotyczą, znajdującym się w Unii, a RODO będzie miało zastosowanie do powiązanych czynności przetwarzania.

c) Monitorowanie zachowania osób, których dane dotyczą

Drugim rodzajem działalności powodującym zastosowanie art. 3 ust. 2 jest monitorowanie zachowania osób, których dane dotyczą, o ile zachowanie to ma miejsce w Unii.

Zgodnie z motywem 24 „[p]rzetwarzanie danych osobowych znajdujących się w Unii osób, których dane dotyczą, przez administratora lub podmiot przetwarzający, którzy nie mają jednostki organizacyjnej w Unii, powinno podlegać niniejszemu rozporządzeniu także w przypadkach, gdy wiąże się z monitorowaniem zachowania takich osób, których dane dotyczą, o ile zachowanie to ma miejsce w Unii".

Aby zastosowanie miały przepisy RODO na podstawie art. 3 ust. 2 lit. b) monitorowane zachowanie musi odnosić się w pierwszej kolejności do osoby, której dane dotyczą, w Unii oraz – jako łączne kryterium – monitorowane zachowanie musi mieć miejsce na terytorium Unii.

Charakter czynności przetwarzania, którą można uznać za monitorowanie zachowania określono w motywie 24, zgodnie z którym „[a]by stwierdzić, czy czynność przetwarzania można uznać za »monitorowanie zachowania« osób, których dane dotyczą, należy ustalić, czy osoby fizyczne są obserwowane w internecie, w tym także czy później potencjalnie stosowane są techniki przetwarzania danych polegające na profilowaniu osoby fizycznej, w szczególności w celu podjęcia decyzji jej dotyczącej lub przeanalizowania lub prognozowania jej osobistych preferencji, zachowań i postaw".

Chociaż motyw 24 odnosi się wyłącznie do monitorowania zachowania poprzez obserwowanie osoby w internecie, EROD uważa, że przy ustalaniu, czy przetwarzanie jest równoznaczne z monitorowaniem zachowania powinno się brać pod uwagę również obserwowanie za pośrednictwem innych rodzajów sieci lub technologii wiążących się z przetwarzaniem danych osobowych, na przykład za pośrednictwem urządzeń do noszenia na ciele i innych urządzeń inteligentnych.

W przeciwieństwie do przepisu art. 3 ust. 2 lit. a), ani w art. 3 ust. 2 lit. b), ani w motywie 24 nie wprowadzono wyraźnie niezbędnego zakresu „zamiaru kierowania" ze strony administratora danych lub podmiotu przetwarzającego w celu ustalenia, czy działalność monitorowania spowoduje obowiązek stosowania przepisów RODO do czynności przetwarzania. Użycie słowa „monitorowanie" oznacza jednak, że administrator danych ma na uwadze szczególny cel gromadzenia i późniejszego ponownego wykorzystania odpowiednich danych na temat zachowania danej osoby fizycznej w UE. Europejska Rada Ochrony Danych nie uważa, by każde gromadzenie online danych osobowych osób fizycznych w UE lub ich analiza były automatycznie uznawane za „monitorowanie". Należy wziąć pod uwagę cel przetwarzania danych przez administratora danych, a zwłaszcza każdą późniejszą analizę behawioralną lub techniki profilowania dotyczące tych danych. EROD bierze pod uwagę brzmienie motywu 24, który wskazuje, że w celu ustalenia, czy przetwarzanie obejmuje monitorowanie zachowania osoby, której dane dotyczą, kluczową kwestią jest obserwowanie osób fizycznych w internecie, w tym potencjalne późniejsze stosowanie technik profilowania.

W sytuacji, gdy administrator danych lub podmiot przetwarzający monitorują zachowanie osób, których dane dotyczą, przebywających w Unii, art. 3 ust. 2 lit. b) może mieć zatem zastosowanie do szerokiego zakresu działań monitorowania, w tym w szczególności do:

- Reklamy behawioralnej
- Działań w zakresie geolokalizacji, zwłaszcza w celach marketingowych
- Obserwowania przez internet za pomocą plików cookie lub innych technik śledzenia takich jak pobieranie odcisków palców
- Zindywidualizowanych usług online w zakresie diety i analizy zdrowia
- CCTV
- Badania rynku i innych badań behawioralnych w oparciu o poszczególne profile
- Monitorowania lub regularnego składania sprawozdań na temat stanu zdrowia danej osoby fizycznej

Przykład 17: Przedsiębiorstwo konsultingowe w branży detalicznej z siedzibą w USA świadczy usługi doradcze na temat rozplanowania sklepów detalicznych w centrum handlowym we Francji, w oparciu o analizę danych dotyczących przemieszczania się klientów na terenie całego ośrodka gromadzonych za pomocą monitorowania lokalizacji za pośrednictwem sieci Wi-Fi.

Analiza przemieszczania się klientów w centrum poprzez monitorowanie lokalizacji za pośrednictwem sieci Wi-Fi będzie miała charakter monitorowania zachowań osób fizycznych. W tym przypadku zachowanie osób, których dane dotyczą, ma miejsce w Unii, ponieważ centrum handlowe jest zlokalizowane we Francji. Przedsiębiorstwo konsultingowe jako administrator danych jest zatem objęte zakresem stosowania RODO w odniesieniu do przetwarzania takich danych w tym celu zgodnie z jego art. 3 ust. 2 lit. b).

Zgodnie z art. 27 administrator danych będzie musiał wyznaczyć przedstawiciela w Unii.

Przykład 18: Twórca aplikacji mający siedzibę w Kanadzie i niemający jednostki organizacyjnej w Unii monitoruje zachowanie osoby, której dane dotyczą, przebywającej w Unii, podlega zatem przepisom

RODO zgodnie z art. 3 ust. 2 lit. b). Twórca korzysta z usług podmiotu przetwarzającego znajdującego się w Stanach Zjednoczonych do celów optymalizacji i utrzymania aplikacji.

W tym przypadku kanadyjski administrator danych ma obowiązek korzystania z usług wyłącznie odpowiednich podmiotów przetwarzających oraz zapewnienia wprowadzania odpowiednich zobowiązań wynikających z RODO do umowy lub instrumentu prawnego, zawartych z podmiotem przetwarzającym znajdującym się w Stanach Zjednoczonych, zgodnie z art. 28.

d) Podmiot przetwarzający niemający jednostki organizacyjnej w Unii

Czynności przetwarzania „związane" z ukierunkowaną działalnością, która powoduje stosowanie art. 3 ust. 2, wchodzą w terytorialny zakres stosowania RODO. Europejska Rada Ochrony Danych uważa, że musi istnieć związek między czynnością przetwarzania a oferowaniem towarów lub usług, ale znaczenie ma zarówno przetwarzanie przez administratora danych jak i przez podmiot przetwarzający i należy je uwzględnić.

Jeżeli podmiot przetwarzający nie ma jednostki organizacyjnej w Unii, w celu ustalenia, czy przetwarzanie przez niego danych może podlegać RODO zgodnie z art. 3 ust. 2, należy zastanowić się, czy przetwarzanie danych przez podmiot przetwarzający „jest związane" z ukierunkowaną działalnością administratora danych.

Europejska Rada Ochrony Danych uważa, że w przypadku, gdy czynności przetwarzania przez administratora danych są związane z oferowaniem towarów lub usług albo monitorowaniem zachowania osób fizycznych w Unii („kierowanie"), każdy podmiot przetwarzający zobowiązany do dokonywania takiej czynności przetwarzania w imieniu administratora danych wchodzi w zakres stosowania RODO na mocy art. 3 ust. 2 w odniesieniu do tego przetwarzania.

„Ukierunkowany" charakter czynności przetwarzania jest powiązany z jej celami i środkami; decyzję o tym, aby skierować działalność do osób fizycznych w Unii może podjąć jedynie podmiot działający jako administrator danych. Taka interpretacja nie wyklucza, że podmiot przetwarzający może aktywnie uczestniczyć w czynnościach przetwarzania związanych z realizacją kryterium „kierowania" (tj. podmiot przetwarzający oferuje towary lub usługi lub prowadzi działania monitorujące w imieniu administratora danych i na jego polecenie).

W związku z tym EROD uważa, że należy skupić się na związku między czynnościami przetwarzania dokonywanymi przez podmiot przetwarzający a ukierunkowaną działalnością prowadzoną przez administratora danych.

Przykład 19: Brazylijskie przedsiębiorstwo sprzedaje w internecie składniki żywności i lokalne przepisy, udostępniając je osobom w Unii, reklamując te produkty i oferując dostawę we Francji, Hiszpanii i Portugalii. W tym kontekście przedsiębiorstwo zleca podmiotowi przetwarzającemu, również z siedzibą w Brazylii, opracowanie specjalnych ofert dla klientów we Francji, Hiszpanii i Portugalii na podstawie ich wcześniejszych zamówień oraz związane z tym przetwarzanie danych.

Czynności przetwarzania dokonywane przez podmiot przetwarzający na polecenie administratora danych są związane z oferowaniem towarów osobie, których dane dotyczą, przebywającej w Unii. Ponadto, rozwijając te zindywidualizowane oferty, podmiot przetwarzający bezpośrednio monitoruje osoby, których dane dotyczą, przebywające w UE. Przetwarzanie danych przez podmiot przetwarzający jest zatem objęte przepisami RODO, zgodnie z art. 3 ust. 2.

Przykład 20: Amerykańskie przedsiębiorstwo opracowało aplikację dotyczącą zdrowia i stylu życia, dzięki której użytkownicy mogą rejestrować w amerykańskim przedsiębiorstwie swoje osobiste wskaźniki (czas snu, wagę, ciśnienie tętnicze, tętno itd.). Następnie aplikacja udziela użytkownikom codziennych porad na temat żywności i podaje zalecenia sportowe. Przetwarzania danych dokonuje amerykański administrator danych. Aplikacja jest dostępna dla osób fizycznych w Unii i jest przez nie wykorzystywana. Do celów przechowywania danych amerykańskie przedsiębiorstwo korzysta z usług podmiotu przetwarzającego z siedzibą w Stanach Zjednoczonych (dostawca usług w chmurze).
W zakresie, w jakim amerykańskie przedsiębiorstwo monitoruje zachowanie osób fizycznych w UE w trakcie obsługi aplikacji dotyczącej zdrowia i stylu życia, „kieruje" ono swoją działalność do osób w UE, a przetwarzanie danych osobowych osób fizycznych w UE będzie objęte zakresem stosowania RODO na mocy art. 3 ust. 2.

W trakcie przetwarzania na polecenie i w imieniu amerykańskiego przedsiębiorstwa, amerykański dostawca usług w chmurze/podmiot przetwarzający prowadzi przetwarzanie „związane z" działalnością kierowaną przez administratora danych do osób fizycznych w UE. Takie przetwarzanie danych przez podmiot przetwarzający w imieniu administratora danych wchodzi w zakres stosowania RODO na mocy art. 3 ust. 2.

Przykład 21: Tureckie przedsiębiorstwo oferuje kulturalne wycieczki turystyczne na Bliskim Wschodzie z udziałem przewodników mówiących z języku angielskim, francuskim i hiszpańskim. Reklama i oferta wycieczek dostępne są przede wszystkim na stronie internetowej prowadzonej w trzech językach, umożliwiającej rezerwację online i płatność w euro i funtach szterlingach. W celach marketingowych i poszukiwania możliwości handlowych przedsiębiorstwo zleca podmiotowi przetwarzającemu, centrum telefonicznemu z siedzibą w Tunezji, kontaktowanie się z byłymi klientami w Irlandii, Francji, Belgii i Hiszpanii w celu uzyskania informacji zwrotnych na temat ich wcześniejszych podróży oraz poinformowania ich o nowych ofertach i miejscach.
Administrator danych „ukierunkowuje" swoją działalność poprzez oferowanie swoich usług osobom fizycznym w UE, a przetwarzanie przez niego będzie objęte zakresem stosowania art. 3 ust. 2.

Czynności przetwarzania tunezyjskiego podmiotu przetwarzającego, który promuje usługi administratorów danych wśród osób fizycznych w UE są również związane z oferowaniem usług przez administratora danych i w związku z tym wchodzą w zakres stosowania art. 3 ust. 2. Ponadto w tym konkretnym przypadku tunezyjski podmiot przetwarzający aktywnie uczestniczy w czynnościach przetwarzania związanych ze spełnianiem kryterium „kierowania", oferując usługi w imieniu i na zlecenie tureckiego administratora danych.

e) Współdziałanie z innymi przepisami RODO i pozostałymi przepisami

Europejska Rada Ochrony Danych dokona również dalszej oceny zależności między stosowaniem terytorialnego zakresu stosowania RODO zgodnie z art. 3 a przepisami dotyczącymi międzynarodowego przekazywania danych zgodnie z rozdziałem V. W razie konieczności może wydać dodatkowe wytyczne w tym zakresie.

Administratorzy danych lub podmioty przetwarzające niemający jednostki organizacyjnej w UE będą zobowiązani do przestrzegania przepisów krajowych obowiązujących w swoich państwach trzecich w odniesieniu do przetwarzania danych osobowych. Jeżeli jednak przetwarzanie dotyczy działalności skierowanej do osób fizycznych w Unii zgodnie z art. 3 ust. 2, administrator danych, oprócz stosowania przepisów krajowych swojego państwa, będzie zobowiązany do przestrzegania RODO. Przepisy RODO

będą miały zastosowanie niezależnie od tego, czy przetwarzanie danych odbywa się zgodnie z obowiązkiem prawnym w takim państwie trzecim, czy po prostu z wyboru administratora danych.

3 PRZETWARZANIE W MIEJSCU, W KTÓRYM NA MOCY PRAWA MIĘDZYNARODOWEGO PUBLICZNEGO MA ZASTOSOWANIE PRAWO PAŃSTWA CZŁONKOWSKIEGO

Artykuł 3 ust. 3 stanowi, że „[n]iniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych przez administratora niemającego jednostki organizacyjnej w Unii, ale posiadającego jednostkę organizacyjną w miejscu, w którym na mocy prawa międzynarodowego publicznego ma zastosowanie prawo państwa członkowskiego". Motyw 25 rozszerza ten przepis i stanowi, że „[n]iniejsze rozporządzenie powinno mieć zastosowanie do administratora niemającego jednostki organizacyjnej w Unii także w przypadkach, gdy na mocy prawa międzynarodowego publicznego stosuje się prawo państwa członkowskiego, na przykład na terenie misji dyplomatycznej lub placówki konsularnej państwa członkowskiego".

Europejska Rada Ochrony Danych uważa zatem, że RODO ma zastosowanie do przetwarzania danych osobowych przez ambasady i konsulaty państw członkowskich UE znajdujące się poza terytorium UE, ponieważ takie przetwarzanie wchodzi w zakres stosowania RODO na podstawie art. 3 ust. 3. Placówka dyplomatyczna lub konsularna danego państwa członkowskiego, jako administrator danych lub podmiot przetwarzający, podlegałyby wówczas wszystkim stosownym przepisom RODO, w tym przepisom dotyczącym praw osoby, której dane dotyczą, ogólnym obowiązkom dotyczącym administratora danych i podmiotu przetwarzającego oraz przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych.

Przykład 22: Niderlandzki konsulat w Kingston, Jamajka, otwiera internetowy proces rekrutacji miejscowego personelu w celu wsparcia swojej administracji.

O ile konsulat niderlandzki w Kingston na Jamajce, nie ma jednostki organizacyjnej w Unii, o tyle fakt, że jest to placówka konsularna kraju UE, w którym zastosowanie ma prawo państwa członkowskiego na mocy prawa międzynarodowego publicznego, sprawia, że zgodnie z art. 3 ust. 3, do przetwarzania danych osobowych zastosowanie mają przepisy RODO.

Przykład 23: Niemiecki statek wycieczkowy poruszający się po wodach międzynarodowych przetwarza dane gości na pokładzie w celu dostosowania oferty rozrywkowej rejsów wycieczkowych.
Chociaż statek znajduje się poza terytorium Unii, na wodach międzynarodowych, fakt, że jest to zarejestrowany w Niemczech statek wycieczkowy oznacza, że na mocy prawa międzynarodowego publicznego, zgodnie z art. 3 ust. 3, zastosowanie do przetwarzania danych osobowych mają przepisy RODO.

Chociaż nie jest to związane ze stosowaniem art. 3 ust. 3, innym przypadkiem jest sytuacja, w której na mocy prawa międzynarodowego niektóre podmioty, organy lub organizacje mające jednostkę organizacyjną w Unii korzystają z przywilejów i immunitetów, takich jak te określone w Konwencji wiedeńskiej o stosunkach dyplomatycznych z 1961 r.[27], Konwencji wiedeńskiej o stosunkach konsularnych z 1963 r. lub umowach w sprawie siedziby zawartych między organizacjami międzynarodowymi a ich państwami przyjmującymi w Unii. W tym względzie EROD przypomina, że

[27] http://legal.un.org/ilc/texts/instruments/english/conventions/9_1_1961.pdf

stosowanie RODO pozostaje bez uszczerbku dla przepisów prawa międzynarodowego, takich jak przepisy regulujące przywileje i immunitety misji dyplomatycznych i urzędów konsularnych, a także organizacji międzynarodowych niebędących placówkami i organizacjami UE. Jednocześnie należy przypomnieć, że każdy administrator danych lub podmiot przetwarzający, który podlega przepisom RODO w odniesieniu do danej czynności przetwarzania oraz wymienia dane osobowe z takimi podmiotami, organami i organizacjami, musi przestrzegać przepisów RODO, w tym w stosownych przypadkach, jego przepisów dotyczących przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych.

4 PRZEDSTAWICIELE ADMINISTRATORÓW LUB PODMIOTÓW PRZETWARZAJĄCYCH NIEMAJĄCYCH JEDNOSTKI ORGANIZACYJNEJ W UNII

Administratorzy danych lub podmioty przetwarzające, którzy podlegają przepisom RODO zgodnie z jego art. 3 ust. 2, są zobowiązani do wyznaczenia przedstawiciela w Unii. Jeżeli administrator danych lub podmiot przetwarzający niemający jednostki organizacyjnej w Unii, podlegający jednak przepisom RODO, nie wyznaczy przedstawiciela w Unii, naruszy przepisy rozporządzenia.

Przepis ten nie jest całkowicie nowy, ponieważ dyrektywa 95/46/WE przewidywała podobne zobowiązanie. Zgodnie z przepisami dyrektywy, przepis ten dotyczył administratorów danych, którzy nie prowadzą działalności gospodarczej na terytorium Wspólnoty, a do celów przetwarzania danych osobowych wykorzystują środki, zarówno zautomatyzowane jak i inne, znajdujące się na terytorium wymienionego państwa członkowskiego. Ogólne rozporządzenie o ochronie danych nakłada obowiązek wyznaczenia przedstawiciela w Unii na każdego administratora danych lub podmiot przetwarzający objętych zakresem stosowania art. 3 ust. 2, chyba że spełniają oni kryteria odstępstwa określone w art. 27 ust. 2. W celu ułatwienia stosowania tego przepisu EROD uważa, że konieczne jest sporządzenie dalszych wytycznych w sprawie procesu wyznaczania, ustanowienia, zobowiązań i obowiązków przedstawiciela w Unii zgodnie z art. 27.

Warto zauważyć, że administrator danych lub podmiot przetwarzający niemający jednostki organizacyjnej w Unii, którzy wyznaczyli na piśmie swojego przedstawiciela w Unii zgodnie z art. 27 RODO, nie wchodzą w zakres stosowania art. 3 ust. 1, co oznacza, że obecność przedstawiciela w Unii nie stanowi „jednostki organizacyjnej" administratora danych lub podmiotu przetwarzającego na mocy art. 3 ust. 1.

a) Wyznaczenie przedstawiciela

W motywie 80 wyjaśniono, że „[a]dministrator lub podmiot przetwarzający powinien wyznaczyć przedstawiciela w wyraźny sposób za pomocą pisemnego upoważnienia do podejmowania działań w jego imieniu w odniesieniu do obowiązków administratora lub podmiotu przetwarzającego wynikających z niniejszego rozporządzenia. *Wyznaczenie przedstawiciela nie wpływa na obowiązki lub odpowiedzialność prawną administratora lub podmiotu przetwarzającego wynikającą z niniejszego rozporządzenia. Przedstawiciel powinien wykonywać swoje zadania zgodnie z upoważnieniem otrzymanym od administratora lub podmiotu przetwarzającego, w tym współpracować z właściwymi organami nadzorczymi w odniesieniu do wszelkich działań służących zapewnieniu przestrzegania niniejszego rozporządzenia".*

Pisemne upoważnienie, o którym mowa w motywie 80 reguluje zatem stosunki i obowiązki między przedstawicielem w Unii a administratorem danych lub podmiotem przetwarzającym mającym

siedzibę poza Unią, nie wpływając jednocześnie na obowiązki ani odpowiedzialność administratora danych lub podmiotu przetwarzającego. Przedstawiciel w Unii może być osobą fizyczną lub prawną mającą siedzibę w Unii, zdolną do reprezentowania administratora danych lub podmiotu przetwarzającego mających siedzibę poza Unią w odniesieniu do ich odpowiednich obowiązków wynikających z RODO.

W praktyce funkcję przedstawiciela w Unii można wykonywać na podstawie umowy o świadczenie usług zawartej z osobą fizyczną lub organizacją, a zatem może ją pełnić szereg podmiotów handlowych i niekomercyjnych, takich jak kancelarie prawne, firmy konsultingowe, przedsiębiorstwa prywatne itp., pod warunkiem że podmioty te mają siedzibę w Unii. Jeden przedstawiciel może również działać w imieniu kilku administratorów danych i podmiotów przetwarzających spoza UE.

Jeżeli przedsiębiorstwo lub inny rodzaj organizacji przejmuje funkcję przedstawiciela, zaleca się przypisanie pojedynczej osoby jako osoby wyznaczonej do kontaktów i osoby „odpowiedzialnej" za każdego reprezentowanego administratora danych lub podmiotu przetwarzającego. Zasadniczo przydatne byłoby również zawarcie tych punktów w umowie o świadczenie usług.

Zgodnie z RODO, Europejska Rada Ochrony Danych potwierdza, że w przypadku gdy kilka czynności przetwarzania administratora danych lub podmiotu przetwarzającego wchodzi w zakres stosowania art. 3 ust. 2 RODO (i nie ma zastosowania żadne odstępstwo określone w art. 27 ust. 2 RODO), administrator danych lub podmiot przetwarzający nie musi wyznaczać kilku przedstawicieli do każdej odrębnej czynności przetwarzania wchodzącej w zakres stosowania art. 3 ust. 2. Europejska Rada Ochrony Danych nie uznaje funkcji przedstawiciela w Unii za funkcję równą funkcji zewnętrznego inspektora ochrony danych, który miałby siedzibę w Unii. W art. 38 ust. 3 ustanowiono pewne podstawowe gwarancje mające pomóc w zapewnieniu, aby inspektorzy ochrony danych mogli wykonywać swoje zadania z zachowaniem stosownej autonomii w ramach swojej organizacji. W szczególności administratorzy lub podmioty przetwarzające zapewniają, by inspektor ochrony danych „nie otrzymywał instrukcji dotyczących wykonywania [swoich] zadań". W motywie 97 dodano, że „inspektorzy ochrony danych – bez względu na to, czy są pracownikami administratora – powinni być w stanie wykonywać swoje obowiązki i zadania w sposób niezależny"[28]. Taki wymóg zapewnienia wystarczającego stopnia autonomii i niezależności inspektora ochrony danych nie wydaje się zgodny z funkcją przedstawiciela w Unii. Przedstawiciel działa na mocy upoważnienia udzielonego przez administratora danych lub podmiot przetwarzający i będzie działał w jego imieniu, a zatem zgodnie z jego bezpośrednimi instrukcjami[29]. Przedstawiciel jest upoważniony przez administratora danych lub podmiot przetwarzający, których reprezentuje, i w związku z tym wykonując swoje zadania działa w ich imieniu, a taka rola nie może być zgodna z rolą inspektora ochrony danych polegającą na niezależnym wykonywaniu swoich obowiązków i zadań.

Ponadto, aby uzupełnić swoją interpretację, EROD przywołuje stanowisko przyjęte już przez Grupę Roboczą Art. 29, w którym podkreśla się, że „konflikt interesów może powstać, gdy zewnętrzny DPO zostanie poproszony o reprezentowanie administratora lub podmiotu przetwarzającego przed sądem w sprawie dotyczącej ochrony danych osobowych"[30].

[28] Wytyczne Grupy Roboczej Art. 29 dotyczące inspektorów ochrony danych („DPO"), WP 243 rev.01 – zatwierdzone przez Europejską Radę Ochrony Danych.

[29] Na przykład, zewnętrzny inspektor ochrony danych działający również w charakterze przedstawiciela w Unii nie może znaleźć się w sytuacji, w której jako przedstawiciel otrzymał polecenie przekazania osobie, której dane dotyczą, decyzji lub środka podjętych przez administratora danych lub podmiot przetwarzający, które – w jego ocenie jako inspektora ochrony danych – są niezgodne z przepisami RODO, i których podjęcia odradzał.

[30] Wytyczne Grupy Roboczej Art. 29 dotyczące inspektorów ochrony danych („DPO"), WP 243 rev.01 – zatwierdzone przez Europejską Radę Ochrony Danych.

Podobnie, biorąc pod uwagę ewentualny konflikt obowiązków i interesów w przypadku postępowań w zakresie egzekwowania prawa, EROD nie uznaje funkcji przedstawiciela administratora danych w Unii za zgodną z rolą podmiotu przetwarzającego w odniesieniu do tego samego administratora danych, zwłaszcza w zakresie przestrzegania ich odpowiednich obowiązków.

O ile w RODO nie nakłada się na administratora danych ani na samego przedstawiciela żadnego obowiązku powiadomienia organu nadzorczego o wyznaczeniu przedstawiciela do sprawowania tej funkcji, EROD przypomina, że zgodnie z art. 13 ust. 1 lit. a) i 14 ust. 1 lit. a), w ramach swoich obowiązków informacyjnych, administratorzy danych przekazują informacje na temat tożsamości ich przedstawiciela w Unii. Informacje te są na przykład zawarte w [informacji o polityce prywatności oraz] informacji wstępnej dostarczanej osobom, których dane dotyczą, w momencie gromadzenia danych. Administrator danych niemający jednostki organizacyjnej w Unii, ale wchodzący w zakres stosowania art. 3 ust. 2 i niezawiadamiający osób, których dane dotyczą, przebywających w Unii o tożsamości swojego przedstawiciela naruszałby swoje obowiązki w zakresie przejrzystości określone w RODO. Takie informacje powinny być ponadto łatwo dostępne dla organów nadzorczych, aby ułatwić nawiązywanie kontaktów na potrzeby współpracy.

Przykład 24: Strona internetowa, o której mowa w przykładzie 12, zlokalizowana i zarządzana w Turcji, oferuje usługi tworzenia, edycji, drukowania i wysyłki spersonalizowanych albumów ze zdjęciami rodzinnymi. Strona internetowa jest dostępna w języku angielskim, francuskim, niderlandzkim i niemieckim, a płatności można dokonywać w euro lub funtach szterlingach. Na stronie wskazano, że albumy fotograficzne dostarcza się wyłącznie pocztą we Francji, krajach Beneluksu i w Niemczech. Strona ta podlega przepisom RODO zgodnie z jego art. 3 ust. 2 lit. a), zatem administrator danych ma obowiązek wyznaczenia przedstawiciela w Unii.

Przedstawiciel musi mieć siedzibę w jednym z państw członkowskich, w których oferowana usługa jest dostępna, w tym przypadku we Francji, Belgii, Holandii, Luksemburgu lub Niemczech. Imię i nazwisko oraz dane kontaktowe administratora danych i jego przedstawiciela w Unii muszą stanowić część informacji udostępnianych przez internet osobom, których dane dotyczą, w momencie, gdy zaczynają oni korzystać z usługi, tworząc album fotograficzny. Na stronie internetowej musi pojawić się również ogólna informacja o polityce prywatności.

b) Odstępstwa od obowiązku wyznaczenia[31]

O ile zastosowanie art. 3 ust. 2 pociąga za sobą obowiązek wyznaczenia przedstawiciela w Unii dla administratorów danych lub podmiotów przetwarzających mających siedzibę poza Unią, o tyle art. 27 ust. 2 przewiduje odstępstwo od obowiązkowego wyznaczenia przedstawiciela w Unii w dwóch odrębnych przypadkach:

- „przetwarzania, które ma charakter sporadyczny, nie obejmuje – na dużą skalę – przetwarzania szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1, ani przetwarzania danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10" i „jest mało prawdopodobne, by ze względu na swój charakter, kontekst, zakres i cele powodowało ryzyko naruszenia praw lub wolności osób fizycznych".

Zgodnie ze stanowiskami zajmowanymi wcześniej przez Grupę Roboczą Art. 29, EROD uważa, że czynność przetwarzania może być uważana za „sporadyczną", jeżeli nie jest prowadzona

[31] Podstawę do zastosowania odstępstwa od obowiązku wyznaczenia może stanowić część kryteriów i interpretacja określone w wytycznych Grupy Roboczej Art. 29, WP243 rev.1 (inspektor ochrony danych), zatwierdzonych przez EROD.

systematycznie i odbywa się poza regularną działalnością administratora lub podmiotu przetwarzającego[32].

Ponadto, mimo iż w RODO nie określono, co stanowi przetwarzanie na dużą skalę, Grupa Robocza Art. 29 zaleciła wcześniej w swoich wytycznych WP243 dotyczących inspektorów ochrony danych (DPO), aby przy ustalaniu, czy przetwarzanie odbywa się na dużą skalę, wziąć pod uwagę w szczególności następujące czynniki: liczbę osób, których dane dotyczą – wyrażoną jako konkretną wartość albo procent określonej grupy społeczeństwa; zakres przetwarzanych danych osobowych; okres, przez jaki dane są przetwarzane; zakres geograficzny czynności przetwarzania[33].

Ponadto EROD podkreśla, że odstępstwo od obowiązku wyznaczenia, o którym mowa w art. 27, odnosi się do przetwarzania, w odniesieniu do którego „jest mało prawdopodobne, by powodowało ryzyko naruszenia praw lub wolności osób fizycznych"[34], a tym samym nie ogranicza zastosowania odstępstwa do przetwarzania, w odniesieniu do którego jest mało prawdopodobne, by powodowało wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Zgodnie z motywem 75 przy ocenie ryzyka naruszenia praw i wolności osób, których dane dotyczą, należy wziąć pod uwagę zarówno prawdopodobieństwo, jak i powagę zagrożeń.

lub;

- przetwarzania dokonuje „organ lub podmiot publiczny";

Oceny czy podmiot mający siedzibę poza Unią można zakwalifikować jako „organ lub podmiot publiczny" dokonują *in concreto* i w poszczególnych przypadkach organy nadzorcze[35]. EROD zauważa, że z uwagi na charakter swoich zadań i misji przypadki, w których organ lub podmiot publiczny w państwie trzecim oferują towary lub usługi osobom, których dane dotyczą, przebywającym w Unii lub monitorują ich zachowanie mające miejsce w Unii, są raczej ograniczone. c) ***Jednostka organizacyjna w państwie członkowskim, w którym przebywają osoby, których dane dotyczą, których dane osobowe są przetwarzane***

Zgodnie z art 27 ust. 3 „[p]rzedstawiciel musi mieć siedzibę w państwie członkowskim, w którym przebywają osoby, których dane dotyczą, których dane osobowe są przetwarzane w związku z oferowaniem im towarów lub usług lub których zachowanie jest monitorowane". W przypadku gdy znaczna część osób, których dane dotyczą, a których dane osobowe są przetwarzane, znajduje się w jednym z państw członkowskich, EROD zaleca, tytułem dobrych praktyk, by przedstawiciel miał siedzibę w tym samym państwie członkowskim. Przedstawiciel musi być jednak łatwo dostępny dla osób, których dane dotyczą, w państwach członkowskich, w których nie ma on siedziby, a w których oferowane są usługi lub towary, lub w których monitorowane jest ich zachowanie.

Europejska Rada Ochrony Danych potwierdza, że kryterium ustanowienia przedstawiciela w Unii jest miejsce, w którym znajdują się osoby, których dane dotyczą, których dane osobowe są przetwarzane.

[32] Stanowisko Grupy Roboczej Art. 29 w sprawie wyjątków od obowiązku prowadzenia rejestru czynności przetwarzania zgodnie z artykułem 30 ust. 5 RODO.
[33] Wytyczne Grupy Roboczej Art. 29 dotyczące inspektorów ochrony danych („DPO"), przyjęte w dniu 13 grudnia 2016 r., ostatnio zmienione i przyjęte w dniu 5 kwietnia 2017 r., WP 243 rev.01 – zatwierdzone przez Europejską Radę Ochrony Danych.
[34] Artykuł 27 ust. 2 lit. a) RODO.
[35] W RODO nie zdefiniowano czym jest „organ lub podmiot publiczny". Zdaniem EROD pojęcie to należy określić w prawie krajowym. W związku z tym organy i podmioty publiczne obejmują władze krajowe, jednostki samorządu lokalnego i regionalnego, ale pojęcie to, zgodnie z obowiązującym prawem krajowym, obejmuje zazwyczaj również szereg innych podmiotów prawa publicznego.

Miejsce przetwarzania, nawet przez podmiot przetwarzający mający jednostkę organizacyjną w innym państwie członkowskim, nie jest tu istotnym czynnikiem decydującym o lokalizacji przedstawiciela.

Przykład 25: Indyjskie przedsiębiorstwo farmaceutyczne, które nie jest ani obecne w Unii, ani nie ma jednostki organizacyjnej w Unii, podlegające przepisom RODO zgodnie z art. 3 ust. 2, sponsoruje badania kliniczne prowadzone przez badaczy (szpitale) w Belgii, Luksemburgu i Holandii. Większość pacjentów uczestniczących w badaniach klinicznych znajduje się w Belgii.

Indyjskie przedsiębiorstwo farmaceutyczne jako administrator danych wyznacza przedstawiciela w Unii, który ma siedzibę w jednym z trzech państw członkowskich, w których pacjenci, jako osoby, których dane dotyczą, uczestniczą w badaniu klinicznym (Belgia, Luksemburg lub Holandia). Ponieważ większość pacjentów to mieszkańcy Belgii, zaleca się, aby przedstawiciel miał swoją siedzibę w Belgii. W takim przypadku przedstawiciel w Belgii powinien jednak być łatwo dostępny dla osób, których dane dotyczą, oraz organów nadzorczych w Holandii i Luksemburgu.

W tym konkretnym przypadku przedstawiciel w Unii może być przedstawicielem prawnym sponsora w Unii zgodnie z art. 74 rozporządzenia (UE) 536/2014 w sprawie badań klinicznych pod warunkiem, że nie działa on jako podmiot przetwarzający dane w imieniu sponsora badań klinicznych, że posiada siedzibę w jednym z trzech państw członkowskich oraz że obie te funkcje podlegają poszczególnym ramom prawnym i są zgodnie z nimi wykonywane.

c) Obowiązki i zadania przedstawiciela

Przedstawiciel w Unii działa w imieniu administratora danych lub podmiotu przetwarzającego, którego reprezentuje w zakresie obowiązków administratora danych lub podmiotu przetwarzającego wynikających z RODO. Oznacza to w szczególności obowiązki związane z wykonywaniem praw osób, których dane dotyczą, i dlatego – jak stwierdzono powyżej – tożsamość i dane kontaktowe przedstawiciela muszą być przekazywane osobom, których dane dotyczą, zgodnie z art. 13 i 14. O ile sam przedstawiciel nie jest odpowiedzialny za przestrzeganie praw osób, których dane dotyczą, musi on ułatwiać komunikację między osobami, których dane dotyczą, a administratorem danych lub podmiotem przetwarzającym, których reprezentuje, aby wykonywanie praw przez osoby, których dane dotyczą, było skuteczne.

Zgodnie z art. 30 przedstawiciel administratora danych lub podmiotu przetwarzającego prowadzi w szczególności rejestr czynności przetwarzania pod nadzorem administratora danych lub podmiotu przetwarzającego. Europejska Rada Ochrony Danych uważa, że o ile prowadzenie tego rejestru stanowi obowiązek nałożony zarówno na administratora danych lub podmiot przetwarzający, jak również na przedstawiciela, administrator danych lub podmiot przetwarzający niemający jednostki organizacyjnej w Unii są odpowiedzialni za treść i aktualizację rejestru oraz jednocześnie przekazują swojemu przedstawicielowi wszelkie stosowne i aktualne informacje, tak aby przedstawiciel mógł prowadzić i udostępniać rejestr jednocześnie, to na przedstawicielu spoczywa odpowiedzialność za udostępnienie rejestru zgodnie z art. 27, np. w sytuacji, gdy organ nadzorczy zwróci się do niego zgodnie z art. 27 ust. 4.

Jak wyjaśniono w motywie 80 przedstawiciel powinien wykonywać swoje zadania zgodnie z upoważnieniem otrzymanym od administratora lub podmiotu przetwarzającego, w tym współpracować z właściwymi organami nadzorczymi w odniesieniu do wszelkich działań służących zapewnieniu przestrzegania niniejszego rozporządzenia. W praktyce oznacza to, że organ nadzorczy kontaktuje się z przedstawicielem we wszystkich sprawach związanych z obowiązkami w zakresie przestrzegania przepisów przez administratora danych lub podmiot przetwarzający mający siedzibę poza Unią, a przedstawiciel ułatwia wymianę informacji lub procedur między organem nadzorczym,

który wystąpił z takim wnioskiem, a administratorem danych lub podmiotem przetwarzającym mającym siedzibę poza Unią.

Przedstawiciel w Unii, w razie potrzeby z pomocą zespołu, musi być w stanie skutecznie komunikować się z osobami, których dane dotyczą oraz współpracować z właściwymi organami nadzorczymi. Oznacza to, że komunikacja ta powinna zasadniczo odbywać się w języku lub językach używanych przez organy nadzorcze i zainteresowane osoby, których dane dotyczą, lub, jeżeli wymagałoby to niewspółmiernie dużego wysiłku, przedstawiciel korzysta z innych środków i technik w celu zapewnienia skuteczności komunikacji. Dostępność przedstawiciela jest zatem niezbędna do zapewnienia, by osoby, których dane dotyczą, oraz organy nadzorcze mogły w prosty sposób nawiązać kontakt z administratorem danych lub podmiotem przetwarzającym spoza UE. Zgodnie z motywem 80 i art. 27 ust. 5 wyznaczenie przedstawiciela przez administratora danych lub podmiot przetwarzający nie wpływa na obowiązki lub odpowiedzialność prawną administratora danych lub podmiotu przetwarzającego wynikające z RODO i pozostaje bez uszczerbku dla postępowań, które mogą zostać wszczęte przeciwko administratorowi danych lub podmiotowi przetwarzającemu. W RODO nie ustanowiono zastępczego zobowiązania przedstawiciela w miejsce administratora danych lub podmiotu przetwarzającego, których reprezentuje w Unii.

Należy jednak zauważyć, że pojęcie przedstawiciela zostało wprowadzone właśnie w celu ułatwienia łączności i zapewnienia skutecznego egzekwowania przepisów RODO względem administratorów danych lub podmiotów przetwarzających podlegających przepisom art. 3 ust. 2 RODO. W tym celu zamiarem było umożliwienie organom nadzorczym wszczęcia postępowania w zakresie egzekwowania prawa za pośrednictwem przedstawiciela wyznaczonego przez administratorów danych lub podmioty przetwarzające niemające jednostki organizacyjnej w Unii. Powyższe obejmuje możliwość skierowania przez organy nadzorcze do przedstawiciela środków naprawczych lub administracyjnych kar pieniężnych i sankcji nałożonych na administratora danych lub podmiot przetwarzający niemających jednostki organizacyjnej w Unii zgodnie z art. 58 ust. 2 i art. 83 RODO. Możliwość bezpośredniego pociągnięcia do odpowiedzialności przedstawiciela jest jednak ograniczona do jego bezpośrednich obowiązków, o których mowa w art. 30 i art. 58 ust. 1 lit. a) RODO.

Europejska Rada Ochrony Danych podkreśla ponadto, że art. 50 RODO ma na celu przede wszystkim ułatwienie egzekwowania przepisów w odniesieniu do państw trzecich i organizacji międzynarodowych oraz że obecnie rozważa się opracowanie dalszych mechanizmów współpracy międzynarodowej w tym zakresie.



Wytyczne 2/2018 w sprawie wyjątków określonych w art. 49 rozporządzenia 2016/679

Przyjęte dnia 25 maja 2018 r.

Spis treści

1. UWAGI OGÓLNE 3

2. SZCZEGÓŁOWA WYKŁADNIA PRZEPISÓW ART. 49 6

2.1 Osoba, której dane dotyczą, poinformowana o ewentualnym ryzyku, z którym – ze względu na brak decyzji stwierdzającej odpowiedni stopień ochrony oraz na brak odpowiednich zabezpieczeń – może się dla niej wiązać proponowane przekazanie, wyraźnie wyraziła na nie zgodę – (art. 49 ust. 1 lit. a)) 6

2.1.1 Zgoda musi być wyraźna 6

2.1.2 Zgoda musi dotyczyć konkretnie danego jednorazowego/wielokrotnego przekazania danych 7

2.1.3 Zgoda musi być świadoma, w szczególności osoba udzielająca zgody musi być świadoma ewentualnego ryzyka, z którym może się wiązać przekazanie 7

2.2 Przekazanie niezbędne do wykonania umowy między osobą, której dane dotyczą, a administratorem lub do wprowadzenia w życie środków przedumownych podejmowanych na żądanie osoby, której dane dotyczą (art. 49 ust. 1 lit. b)) 8

2.3 Przekazanie niezbędne do zawarcia lub wykonania umowy zawartej w interesie osoby, których dane dotyczą, między administratorem a inną osobą fizyczną lub prawną (art. 49 ust. 1 lit. c)) 10

2.4 Przekazanie jest niezbędne ze względu na ważne względy interesu publicznego (art. 49 ust. 1 lit. d)) 10

2.5 Przekazanie jest niezbędne do ustalenia, dochodzenia lub ochrony roszczeń (art. 49 ust. 1 lit. e)) 12

2.6 Przekazanie niezbędne do ochrony żywotnych interesów osoby, których dane dotyczą, lub innych osób, jeżeli osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody (art. 49 ust. 1 lit. f)) 13

2.7 Przekazanie danych z publicznego rejestru (art. 49 ust. 1 lit. g) i art. 49 ust. 2) 14

2.8 Ważne prawnie uzasadnione interesy (art. 49 ust. 1 akapit drugi) 15

Europejska Rada Ochrony Danych

Uwzględniając art. 70 ust. 1 lit. j) i e) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE,

PRZYJĘŁA NASTĘPUJĄCE WYTYCZNE:

1. UWAGI OGÓLNE

Niniejszy dokument ma na celu zapewnienie wytycznych dotyczących stosowania art. 49 ogólnego rozporządzenia o ochronie danych (RODO)[1] w sprawie wyjątków w kontekście przekazywania danych osobowych do państw trzecich.

Niniejszy dokument opiera się na dotychczasowej pracy[2] Grupy Roboczej unijnych organów ds. ochrony danych ustanowionej na mocy art. 29 dyrektywy o ochronie danych (Grupa Robocza Art. 29), którą przejęła Europejska Rada Ochrony Danych w odniesieniu do głównych kwestii wynikających ze stosowania wyjątków w kontekście przekazywania danych osobowych do państw trzecich. Dokument ten zostanie poddany przeglądowi i, w razie konieczności, zostanie zaktualizowany w oparciu o praktyczne doświadczenia zdobyte w wyniku stosowania RODO.

Stosując art. 49, należy mieć na uwadze, że zgodnie z art. 44 podmiot przekazujący dane osobowe do państw trzecich lub organizacji międzynarodowych musi również spełniać warunki określone w pozostałych przepisach RODO. Każda czynność przetwarzania musi być zgodna z właściwymi przepisami o ochronie danych, w szczególności z art. 5 i 6. W związku z tym każda czynność musi spełniać dwa warunki: po pierwsze, podstawa prawna wraz ze wszystkimi właściwymi przepisami RODO musi mieć zastosowanie do przetwarzania danych jako takiego; a po drugie, muszą być spełnione przepisy rozdziału V.

Art. 49 ust. 1 stanowi, że w razie braku decyzji stwierdzającej odpowiedni stopień ochrony lub braku odpowiednich zabezpieczeń jednorazowe lub wielokrotne przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej mogą nastąpić wyłącznie pod pewnymi warunkami. Jednocześnie w art. 44 nałożono wymóg, zgodnie z którym wszystkie przepisy rozdziału V należy stosować w sposób zapewniający, by nie został naruszony stopień ochrony osób fizycznych zagwarantowany w RODO. Oznacza to również, że powoływanie się na wyjątki określone w art. 49 nie powinno nigdy prowadzić do sytuacji, w której mogłyby zostać naruszone prawa podstawowe[3].

Grupa Robocza Art. 29, jako podmiot poprzedzający Europejską Radę Ochrony Danych, od dawna zalecała jako najlepszą praktykę podejście wielopłaszczyznowe[4] do przekazywania danych polegające

[1] ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).
[2] Dokument roboczy Grupy Roboczej Art. 29 w sprawie wspólnej wykładni art. 26 ust. 1 dyrektywy 95/46/WE z dnia 24 października 1995 r., przyjęty 25 listopada 2005 r. (WP114).
[3] Dokument roboczy Grupy Roboczej Art. 29, WP 114, s. 9 i dokument roboczy Grupy Roboczej Art. 29 w sprawie nadzoru komunikacji elektronicznej na potrzeby wywiadu i bezpieczeństwa narodowego (WP 228), s. 39.
[4] Grupa Robocza Art. 29, WP 114, s. 9.

na rozważeniu w pierwszej kolejności, czy dane państwo trzecie zapewnia odpowiedni stopień ochrony, oraz na zapewnieniu, by przekazane dane były zabezpieczone w tym państwie trzecim. Jeżeli stopień ochrony nie jest odpowiedni w świetle wszystkich okoliczności, podmiot przekazujący dane powinien zapewnić odpowiednie zabezpieczenia. Podmioty przekazujące dane powinny zatem najpierw skorzystać z możliwości przekazania danych w ramach jednego z mechanizmów określonych w art. 45 i 46 RODO i dopiero w ich braku zastosować wyjątki określone w art. 49 ust. 1.

W związku z tym wyjątki na mocy art. 49 stanowią odstępstwa od ogólnej zasady, zgodnie z którą dane osobowe można przekazywać do państw trzecich wyłącznie wówczas, gdy w danym państwie trzecim zapewniono odpowiedni stopień ochrony lub gdy wprowadzono odpowiednie zabezpieczenia, a osoby, których dane dotyczą, korzystają z egzekwowalnych i skutecznych praw w celu dalszego korzystania z przysługujących im praw podstawowych i zabezpieczeń[5]. W związku z tym i zgodnie z zasadami właściwymi dla prawa europejskiego[6] wyjątki należy interpretować w sposób ścisły, aby wyjątki te nie stawały się regułą[7]. Znajduje to potwierdzenie w brzmieniu tytułu art. 49, który stanowi, że wyjątki należy stosować w szczególnych sytuacjach („Wyjątki w szczególnych sytuacjach").

Rozważając przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych, podmioty przekazujące dane powinny zatem opowiadać się za rozwiązaniami zapewniającymi osobom, których dane dotyczą, gwarancję, że będą nadal korzystały z praw podstawowych i zabezpieczeń, do których są uprawnione, dotyczących przetwarzania ich danych po ich przekazaniu. Ponieważ wyjątki nie zapewniają właściwej ochrony ani odpowiednich zabezpieczeń przekazywanych danych osobowych oraz ponieważ nie ma wymogu uzyskania uprzedniej zgody organów nadzorczych w odniesieniu do przekazań na podstawie wyjątku, przekazywanie danych osobowych do państw trzecich na podstawie wyjątków prowadzi do zwiększonego ryzyka naruszenia praw i wolności osób, których dane dotyczą.

Podmioty przekazujące dane powinny również zdawać sobie sprawę, że w razie braku decyzji stwierdzającej odpowiedni stopień ochrony prawo Unii lub prawo państwa członkowskiego może z uwagi na ważne względy interesu publicznego wyraźnie nakładać ograniczenia na przekazywanie konkretnych kategorii danych osobowych do państwa trzeciego lub organizacji międzynarodowej (art. 49 ust. 5).

Sporadyczne i niepowtarzające się przekazania

Europejska Rada Ochrony Danych wskazuje, że termin „sporadyczne" zastosowano w motywie 111, a wyrażenie „nie jest powtarzalne" zastosowano w wyjątku dotyczącym „ważnych prawnie uzasadnionych interesów" w art. 49 ust. 1 akapit drugi. Wyrażenia te sugerują, że takie przekazania mogą mieć miejsce więcej niż jeden raz, ale nie regularnie, a ich przeprowadzenie wykracza poza regularne działania, na przykład następują w losowych, nieznanych okolicznościach i w uznaniowych odstępach czasu. Na przykład przekazywanie danych, które odbywa się regularnie w ramach stałej

[5] Motyw 114

[6] Grupa Robocza Art. 29, WP 114, s. 7

[7] Zob. dokument roboczy Grupy Roboczej Art. 29, WP 114, s. 7. Trybunał Sprawiedliwości wielokrotnie podkreślał, że „ochrona prawa podstawowego do poszanowania życia prywatnego na poziomie Unii wymaga, aby odstępstwa od ochrony danych osobowych i jej ograniczenia ograniczały się do tego, co absolutnie konieczne" (wyrok z dnia 16 grudnia 2008 r., Satakunnan Markkinapörssi i Satamedia, C 73/07, pkt 56; wyrok z dnia 9 listopada 2010 r., Volker und Markus Schecke i Eifert, C 92/09 i C 93/09, pkt 77; wyrok Digital Rights, pkt 52; wyrok z dnia 6 października 2015 r., Schrems, C 362/14, pkt 92 i wyrok z dnia 21 grudnia 2016 r., Tele2 Sverige AB, C 203/15, pkt 96). Zob. również art. 2 ust. 2 lit. a) protokołu dodatkowego do Konwencji 108 dotyczącego organów nadzoru i transgranicznych przepływów danych, s. 6, dostępnego na stronie https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/181 1)

relacji między podmiotem przekazującym dane a pewnym podmiotem odbierającym dane, można w zasadzie uznać za systematyczne i powtarzalne, w związku z czym nie można stwierdzić, że jest sporadyczne lub niepowtarzające się. Ponadto na przykład przekazanie nie zostanie zwykle uznane za sporadyczne lub powtarzające się, jeżeli podmiotowi odbierającemu dane przyznano bezpośredni dostęp do bazy danych (np. za pośrednictwem interfejsu do programu komputerowego) na zasadach ogólnych.

W motywie 111 rozróżniono wyjątki przez wyraźne stwierdzenie, że wyjątki dotyczące „umowy" i „roszczeń" (art. 49 ust. 1 lit. b). c) i e)) należy ograniczyć do „sporadycznych" przekazań, natomiast takie ograniczenie nie występuje w przypadku „wyjątku w związku z wyraźną zgodą", „wyjątku z uwagi na ważne względy interesu publicznego", „wyjątku z uwagi na żywotne interesy" i „wyjątku dotyczącego rejestru" na podstawie art. 49 ust. 1 lit. a), d), f) i odpowiednio g).

Należy jednak podkreślić, że nawet te wyjątki, które nie zostały wyraźnie ograniczone do „sporadycznych" lub „niepowtarzających się" przekazań, należy interpretować w sposób, który nie jest sprzeczny z charakterem wyjątków jako odstępstw od zasady, zgodnie z którą danych osobowych nie można przekazać do państwa trzeciego, chyba że państwo to zapewni właściwy stopień ochrony danych lub pod warunkiem że zostaną wprowadzone odpowiednie zabezpieczenia[8].

Kryterium niezbędności

Jednym nadrzędnym warunkiem zastosowania kilku wyjątków jest fakt, że przekazanie danych musi być „niezbędne" do realizacji konkretnego celu. Kryterium niezbędności należy stosować do oceny możliwego zastosowania wyjątków określonych w art. 49 ust. 1 lit. b), c), d), e) i f). Zgodnie z tym kryterium podmiot przekazujący dane w UE ocenia, czy przekazanie danych osobowych można uznać za niezbędne do realizacji konkretnego celu, który uzasadnia zastosowanie wyjątku. Więcej informacji na temat konkretnego zastosowania kryterium niezbędności w odniesieniu do każdego z wyjątków można znaleźć w odpowiednich sekcjach poniżej.

Art. 48 w odniesieniu do wyjątków

W art. 48 RODO wprowadzono nowy przepis, który należy brać pod uwagę przy rozważaniu przekazywania danych osobowych. W art. 48 i powiązanym z nim motywie 115 przewidziano, że decyzje organów, sądów lub trybunałów państwa trzeciego nie stanowią same w sobie uzasadnionych podstaw przekazania danych do państw trzecich. W związku z tym każdy przypadek przekazania w odpowiedzi na decyzję organów państwa trzeciego jest zgodny z prawem wyłącznie wówczas, gdy przekazanie jest zgodne z warunkami określonymi w rozdziale V[9].

W przypadkach gdy obowiązuje umowa międzynarodowa, taka jak traktat o wzajemnej pomocy prawnej (MLAT), przedsiębiorstwa UE powinny na ogół odrzucić bezpośrednie wnioski i odesłać organy wzywającego państwa trzeciego do istniejącego traktatu o wzajemnej pomocy prawnej lub obowiązującej umowy.

Taka interpretacja jest również ściśle powiązana z brzmieniem art. 44, w którym określono nadrzędną zasadę mającą zastosowanie do wszystkich przepisów rozdziału V w celu zapewnienia, by stopień ochrony osób fizycznych zagwarantowany w RODO nie został naruszony.

[9] Zob. motyw 115 zdanie 4.

2. SZCZEGÓŁOWA WYKŁADNIA PRZEPISÓW ART. 49

2.1 Osoba, której dane dotyczą, poinformowana o ewentualnym ryzyku, z którym – ze względu na brak decyzji stwierdzającej odpowiedni stopień ochrony oraz na brak odpowiednich zabezpieczeń – może się dla niej wiązać proponowane przekazanie, wyraźnie wyraziła na nie zgodę – art. 49 ust. 1 lit. a)

Ogólne warunki, które zgoda musi spełniać, aby została uznana za ważną, określono w art. 4 pkt 11[10] i w art. 7 RODO[11]. Grupa Robocza Art. 29 zapewnia wskazówki dotyczące tych ogólnych warunków wyrażenia zgody w osobnym dokumencie potwierdzonym przez Europejską Radę Ochrony Danych[12]. Warunki te mają również zastosowanie do zgody w kontekście art. 49 ust. 1 lit. a). Istnieją jednak szczególne, dodatkowe elementy konieczne, aby zgodę można było uznać za ważną podstawę prawną międzynarodowego przekazania danych do państw trzecich lub organizacji międzynarodowych, jak określono w art. 49 ust. 1 lit. a), i niniejszy dokument będzie ich dotyczyć.

W związku z tym przedmiotową sekcję (1) niniejszych wytycznych należy odczytywać w związku z wytycznymi Grupy Roboczej Art. 29 dotyczącymi zgody, potwierdzone przez Europejską Radę Ochrony Danych, które zawierają bardziej szczegółową analizę wyładni ogólnych warunków i kryteriów dotyczących zgody na mocy RODO[13]. Należy również pamiętać, że zgodnie z art. 49 ust. 3 organy publiczne nie mogą powoływać się na ten wyjątek w ramach wykonywania przysługujących im uprawnień publicznych.

W art. 49 ust. 1 lit. a) określono, że przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej może nastąpić w razie braku decyzji stwierdzającej odpowiedni stopień ochrony określonej w art. 45 ust. 3 lub braku odpowiednich zabezpieczeń określonych w art. 46, w tym wiążących reguł korporacyjnych, pod warunkiem że *„osoba, której dane dotyczą, poinformowana o ewentualnym ryzyku, z którym – ze względu na brak decyzji stwierdzającej odpowiedni stopień ochrony oraz na brak odpowiednich zabezpieczeń – może się dla niej wiązać proponowane przekazanie, wyraźnie wyraziła na nie zgodę”*.

2.1.1 Zgoda musi być wyraźna

Zgodnie z art. 4 pkt 11 RODO zgoda powinna być dobrowolna, konkretna, świadoma i jednoznaczna. Jeżeli chodzi o ostatni warunek, przepisy art. 49 ust. 1 lit. a) są bardziej restrykcyjne, ponieważ zawierają wymóg uzyskania „wyraźnej” zgody. Jest to również nowy wymóg w porównaniu z art. 26 ust. 1 lit. a) dyrektywy 95/46/WE, w którym wymagano jedynie „jednoznacznej” zgody. W RODO nałożono wymóg uzyskania wyraźnej zgody w przypadku, gdy może zaistnieć szczególne ryzyko naruszenia ochrony danych, a zatem wymagany jest wysoki stopień indywidualnej ochrony danych osobowych, jak ma to miejsce w przypadku przetwarzania szczególnych kategorii danych (art. 9 ust. 2 lit. a)) i zautomatyzowanych decyzji (art. 22 ust. 2 lit. c)). Takie szczególne ryzyko pojawia się również w kontekście międzynarodowego przekazywania danych.

Więcej wskazówek na temat wymogu dotyczącego wyraźnej zgody oraz pozostałe mające zastosowanie wymogi, które muszą zostać spełnione, aby zgodę można było uznać za ważną, można znaleźć w wytycznych Grupy Roboczej Art. 29 dotyczących zgody potwierdzonych przez Europejską Radę Ochrony Danych[14].

2.1.2 Zgoda musi dotyczyć konkretnie danego jednorazowego/wielokrotnego przekazania danych

Zgodnie z jednym z wymogów ważna zgoda musi być konkretna. Aby zgoda mogła stanowić ważną podstawę przekazania danych na podstawie art. 49 ust. 1 lit. a), musi zostać udzielona konkretnie w odniesieniu do danego jednorazowego lub wielokrotnego przekazania danych.

Terminu „konkretna” użyto w definicji zgody w celu zapewnienia pewnego stopnia kontroli użytkowników i przejrzystości osobie, której dane dotyczą. Termin ten jest również ściśle związany z wymogiem, aby zgoda była „świadoma”.

Z uwagi na fakt, że zgoda musi być konkretna, niekiedy niemożliwe jest uzyskanie uprzedniej zgody osoby, której dane dotyczą, na przyszłe przekazanie w chwili gromadzenia danych, np. jeżeli wystąpienie i szczególne okoliczności przekazania nie są znane w chwili wnioskowania o zgodę, nie można ocenić wpływu przekazania na osobę, której dane dotyczą. Na przykład przedsiębiorstwo UE gromadzi dane swoich klientów w konkretnym celu (dostarczanie towarów), nie rozważając wówczas przekazywania tych danych do osoby trzeciej spoza UE. Kilka lat później to samo przedsiębiorstwo zostaje jednak przejęte przez przedsiębiorstwo spoza UE, które chce przekazać dane osobowe swoich klientów do innego przedsiębiorstwa spoza UE. Aby przekazanie takie było ważne na podstawie wyjątku dotyczącego zgody, osoba, której dane dotyczą, powinna wyrazić zgodę na to konkretne przekazanie w chwili planowania przekazania. W związku z tym zgoda udzielona w czasie gromadzenia danych przez przedsiębiorstwo z UE do celów dostarczania towarów nie jest wystarczająca, aby uzasadnić zastosowanie tego wyjątku w celu przekazania danych osobowych poza UE planowanego w późniejszym terminie.

Podmiot przekazujący dane musi zatem upewnić się, że uzyska konkretną zgodę przed przekazaniem, nawet jeżeli nastąpi to po zgromadzeniu danych. Wymóg ten jest również związany z koniecznością, by zgoda była świadoma. Możliwe jest uzyskanie konkretnej zgody osoby, której dane dotyczą, przed przekazaniem i w chwili gromadzenia danych osobowych, o ile poinformuje się osobę, której dane dotyczą, o konkretnym przekazaniu, a okoliczności przekazania nie zmienią się po wyrażeniu przez osobę, której dane dotyczą, konkretnej zgody. Podmiot przekazujący dane musi zatem upewnić się, że spełniono również wymogi określone w sekcji 1.3 poniżej.

2.1.3 Zgoda musi być świadoma[15], w szczególności osoba udzielająca zgody musi być świadoma ewentualnego ryzyka, z którym może się wiązać przekazanie

Warunek ten jest wyjątkowo istotny, ponieważ wzmacnia i precyzuje ogólny wymóg dotyczący „świadomej” zgody mający zastosowanie do każdej zgody, który ustanowiono w art. 4 pkt 11[16]. Zgodnie z ogólnym wymogiem dotyczącym „świadomej” zgody w przypadku gdy zgoda jest legalną podstawą przekazania danych zgodnie z art. 6 ust. 1 lit. a), należy odpowiednio wcześnie przekazać osobie, której dane dotyczą, informacje o szczególnych okolicznościach przekazania (tj. tożsamość administratora danych, cel przekazania, rodzaj danych, istnienie prawa do cofnięcia zgody, tożsamość lub kategorie odbiorców)[17].

[10] Zgodnie z art. 4 pkt 11 RODO „zgoda” osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.
[11] Dodatkowe wskazówki dotyczące zgody zawarto również w motywach 32, 33, 42 i 43.
[12] Zob. Grupa Robocza Art. 29, Wytyczne dotyczące zgody na mocy rozporządzenia 2016/679 (WP 259).
[13] Tamże.
[14] Tamże.
[15] Należy również przestrzegać ogólnych wymogów dotyczących przejrzystości wyrażonych w art. 13 i 14 RODO. Więcej informacji można znaleźć w Wytycznych dotyczących przejrzystości na mocy rozporządzenia 2016/679 (WP 260).
[16] Zob. Grupa Robocza Art. 29, Wytyczne dotyczące zgody na mocy rozporządzenia 2016/679 (WP 259).
[17] Tamże, s. 13.

Oprócz ogólnego wymogu dotyczącego „świadomej" zgody w przypadku gdy dane osobowe przekazuje się do państwa trzeciego na podstawie art. 49 ust. 1 lit. a), przepis ten wymaga, aby osoby, których dane dotyczą, zostały poinformowane o szczególnym ryzyku wynikającym z faktu, że ich dane zostaną przekazane do państwa, które nie zapewnia właściwiej ochrony, i o niewdrożeniu żadnych odpowiednich zabezpieczeń mających na celu zapewnienie ochrony danych. Przedstawienie tych informacji jest kluczowe, aby umożliwić osobie, której dane dotyczą, wyrażenie zgody przy pełnej wiedzy na temat tych szczególnych okoliczności przekazania, a zatem jeżeli informacji tych nie przedstawiono, wyjątek nie będzie miał zastosowania.

Informacje dostarczone osobom, których dane dotyczą, w celu uzyskania zgody na przekazanie ich danych osobowych do osób trzecich mających siedzibę w państwach trzecich powinny określać również wszystkich odbiorców danych lub kategorie odbiorców, wszystkie państwa, do których dane osobowe są przekazywane, informację, że zgoda stanowi zgodną z prawem podstawę przekazania oraz że państwo trzecie, do którego dane zostaną przekazane, nie zapewnia właściwego poziomu ochrony danych na podstawie decyzji Komisji Europejskiej[18]. Ponadto, jak wspomniano powyżej, należy podać informacje dotyczące ewentualnego ryzyka dla osoby, której dane dotyczą, wynikającego z braku właściwej ochrony w państwie trzecim oraz braku odpowiednich zabezpieczeń. Powiadomienie takie, które można ujednolicić, powinno zawierać na przykład informacje, że w państwie trzecim prawdopodobnie nie istnieje organ nadzorczy ani nie istnieją przepisy dotyczące przetwarzania danych czy też że państwo trzecie może nie gwarantować praw osoby, której dane dotyczą.

W konkretnym przypadku, w którym przekazania dokonuje się po zebraniu danych osobowych od osoby, której dane dotyczą, podmiot przekazujący dane powinien poinformować osobę, której dane dotyczą, o przekazaniu i związanym z nim ryzyku, zanim nastąpi przekazanie, tak aby otrzymać wyraźną zgodę takiej osoby na „proponowane" przekazanie.

Jak wynika z powyższej analizy, w RODO określono rygorystyczne warunki, które trzeba spełnić, aby móc zastosować wyjątek dotyczący zgody. Te rygorystyczne warunki w połączeniu z faktem, że zgoda wyrażona przez osobę, której dane dotyczą, może zostać cofnięta w dowolnym momencie, oznacza, iż zgoda może okazać się niewykonalnym rozwiązaniem długoterminowym do celów przekazywania danych do państw trzecich.

2.2 Przekazanie niezbędne do wykonania umowy między osobą, której dane dotyczą, a administratorem lub do wprowadzenia w życie środków przedumownych podejmowanych na żądanie osoby, której dane dotyczą (art. 49 ust. 1 lit. b))

W świetle motywu 111 przekazanie danych na podstawie tego wyjątku może nastąpić, *„jeżeli przekazywanie jest **sporadyczne** i **niezbędne** w związku z umową […]"*[19].

Co do zasady, chociaż zakres wyjątków związanych z wykonaniem umowy może wydawać się potencjalnie dość szeroki, ograniczają go kryteria dotyczące *„niezbędności"* oraz *„sporadycznego przekazywania"*.

Niezbędność przekazania danych

[18] Ostatni wspomniany wymóg wynika również z obowiązku informowania osób, których dane dotyczą (art. 13 ust. 1 lit. f), art. 14 ust. 1 lit. e)).

[19] Kryterium dotyczące „sporadycznego" przekazywania zawarto w motywie 111 i ma ono zastosowanie do wyjątków określonych w art. 49 ust. 1 lit. b), c) i e).

„Kryterium niezbędności"[20] ogranicza liczbę przypadków, w których można się powołać na art. 49 ust. 1 lit. b)[21]. Wymaga ono ścisłego i znacznego powiązania między przekazaniem danych a celami umowy.

Wyjątku tego nie można zastosować, na przykład jeśli grupa przedsiębiorstw, w celach związanych z działalnością gospodarczą, scentralizowała funkcje zarządzania płatnościami i zasobami ludzkimi w odniesieniu do wszystkich pracowników w państwie trzecim, ponieważ nie istnieje bezpośredni ani obiektywny związek między wykonaniem umowy o pracę a takim przekazaniem[22]. Inne podstawy przekazania, przewidziane w rozdziale V, takie jak standardowe klauzule umowne lub wiążące reguły korporacyjne mogą jednak być odpowiednie w przypadku konkretnego przekazania.

Z drugiej strony przekazanie przez biura podróży danych osobowych dotyczących ich poszczególnych klientów hotelom lub innym partnerom handlowym, do których zwrócono by się w związku z organizacją pobytu tych klientów za granicą, można uznać za niezbędne dla realizacji celów umowy zawartej między biurem podróży a klientem, ponieważ w tym przypadku istnieje wystarczające, ścisłe i znaczne powiązanie między przekazaniem danych a celami umowy (organizacja wycieczek klientów).

Wyjątku tego nie można zastosować do przekazania dodatkowych informacji, które nie są niezbędne do wykonania umowy lub, odpowiednio, do wdrożenia środków przedumownych, których żądała osoba, której dane dotyczą[23]; w przypadku dodatkowych danych wymagane byłyby zatem inne narzędzia.

Sporadyczne przekazania

Dane osobowe można przekazać jedynie na podstawie tego wyjątku, jeśli przekazanie to jest sporadyczne[24]. W poszczególnych przypadkach należałoby ustalić, czy przekazania lub przekazanie danych zostałyby określone jako *„sporadyczne"* lub *„niesporadyczne"*.

W tym przypadku przekazanie można uznać za sporadyczne, na przykład jeśli dane osobowe kierownika sprzedaży, który w ramach swojej umowy o pracę podróżuje do różnych klientów w państwach trzecich, wysyła się do tych klientów w celu zorganizowania spotkań. Przekazanie można również uznać za sporadyczne, jeśli bank znajdujący się w UE przekaże dane osobowe bankowi znajdującemu się w państwie trzecim, aby wykonać zlecenie klienta dotyczące dokonania płatności, o ile przekazanie to nie następuje w ramach stałego stosunku współpracy między oboma bankami.

Przekazania nie zostaną jednak uznane za „sporadyczne" w przypadku, gdy międzynarodowe przedsiębiorstwo organizuje szkolenia w centrum szkoleniowym znajdującym się w państwie trzecim i systematycznie przekazuje dane osobowe pracowników uczęszczających na kurs szkoleniowy (np. dane takie jak imię i nazwisko oraz nazwa stanowiska, ale potencjalnie również informacje na temat wymogów żywieniowych lub ograniczeń ruchowych). Przekazania danych występujące regularnie w ramach stałego stosunku zostałyby uznane za systematyczne i powtarzalne, a zatem wykraczające poza „sporadyczny" charakter. W związku z tym w tym przypadku przekazania danych w ramach stosunku biznesowego nie mogą opierać się na art. 49 ust. 1 lit. b).

[20] Zob. również Opinia 06/2014 Grupy Roboczej Art. 29 w sprawie pojęcia uzasadnionych interesów administratora danych zawartego w art. 7 dyrektywy 95/46/WE (WP 217).

[21] Wymóg dotyczący „niezbędności" można również znaleźć w wyjątkach określonych w art. 49 ust. 1 lit. c)–f).

[22] Ponadto przekazanie nie będzie postrzegane jako sporadyczne (zob. poniżej).

[23] Ogólniej mówiąc, wszystkie wyjątki określone w art. 49 ust. 1 lit. b)–f) dopuszczają możliwość przekazania wyłącznie danych niezbędnych do celu przekazania.

[24] W odniesieniu do ogólnej definicji terminu „sporadyczne" zob. s. 4.

Zgodnie z art. 49 ust. 3 wyjątek ten nie może być stosowany do działalności prowadzonej przez organy publiczne w ramach wykonywania przysługujących im uprawnień publicznych.

2.3 Przekazanie niezbędne do zawarcia lub wykonania umowy zawartej w interesie osoby, których dane dotyczą, między administratorem a inną osobą fizyczną lub prawną (art. 49 ust. 1 lit. c))

Wykładnia tego przepisu jest z konieczności podobna do wykładni art. 49 ust. 1 lit. b); mianowicie przekazanie danych do państwa trzeciego lub organizacji międzynarodowej w przypadku braku decyzji stwierdzającej odpowiedni stopień ochrony na podstawie art. 45 ust. 3 lub odpowiednich zabezpieczeń na podstawie art. 46 można uznać za objęte zakresem wyjątku określonego w art. 49 ust. 1 lit. c) jedynie wtedy, gdy można stwierdzić, że jest ono „niezbędne do zawarcia lub wykonania umowy zawartej między administratorem danych a inną osobą fizyczną lub prawną w interesie osoby, której dane dotyczą".

Oprócz faktu, że przekazanie musi być niezbędne, motyw 111 wskazuje, iż przekazanie danych może nastąpić wyłącznie, *„jeżeli przekazywanie jest* ***sporadyczne*** *i* ***niezbędne*** *w związku z umową […]"*. W związku z tym oprócz *„kryterium niezbędności"* dane osobowe w tym przypadku można przekazać na podstawie tego wyjątku wyłącznie wówczas, gdy przekazanie jest sporadyczne.

Niezbędność przekazania danych i zawarcie umowy w interesie osoby, której dane dotyczą

W przypadku gdy organizacja, w celach związanych z działalnością gospodarczą, zleciła działania w drodze outsourcingu dostawcom usług spoza UE, takie jak zarządzanie płacami, wyjątek ten nie będzie stanowił podstawy do przekazania danych do takich celów, ponieważ nie można ustalić ścisłego i znacznego powiązania między przekazaniem a umową zawartą w interesie osoby, której dane dotyczą, nawet jeśli celem końcowym przekazania jest zarządzanie wynagrodzeniem pracownika[25]. Inne narzędzia przekazywania przewidziane w rozdziale V, takie jak standardowe klauzule umowne lub wiążące reguły korporacyjne, mogą zapewnić odpowiedniejszą podstawę takiego przekazania.

Sporadyczne przekazania

Dane osobowe można ponadto przekazać na podstawie tego wyjątku jedynie wtedy, gdy przekazanie jest sporadyczne, tak jak ma to miejsce w przypadku wyjątku określonego w art. 49 ust. 1 lit. b). W związku z tym, aby ocenić, czy takie przekazanie jest sporadyczne, należy zastosować takie samo kryterium[26].

Ponadto zgodnie z art. 49 ust. 3 wyjątek ten nie może być stosowany do działalności prowadzonej przez organy publiczne w ramach wykonywania przysługujących im uprawnień publicznych[27].

2.4 Przekazanie jest niezbędne ze względu na ważne względy interesu publicznego (art. 49 ust. 1 lit. d))

Wyjątek ten, zazwyczaj zwany „wyjątkiem z uwagi na ważny interes publiczny", jest bardzo podobny do przepisu zawartego w dyrektywie 95/46/WE[28] w art. 26 ust. 1 lit. d), który stanowi, że przekazanie następuje wyłącznie pod warunkiem, że jest konieczne lub wymagane przez prawo z ważnych względów publicznych.

[25] Ponadto przekazanie nie będzie postrzegane jako sporadyczne (zob. poniżej).
[26] W odniesieniu do ogólnej definicji terminu „sporadyczne" zob. s. 4.
[27] Więcej informacji na ten temat można znaleźć w sekcji 1 na s. 5 powyżej.
[28] DYREKTYWA 95/46/WE PARLAMENTU EUROPEJSKIEGO I RADY z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych.

Zgodnie z art. 49 ust. 4 jedynie interesy publiczne uznane w prawie Unii lub w prawie państwa członkowskiego, któremu podlega administrator, mogą doprowadzić do zastosowania tego wyjątku.

Do zastosowania tego wyjątku nie wystarczy jednak wystąpienie o przekazanie danych (na przykład przez organ państwa trzeciego) do celów dochodzenia, które służy interesowi publicznemu państwa trzeciego, który to interes, w abstrakcyjnym sensie, istnieje również w prawie Unii lub państwa członkowskiego. Jeżeli na przykład organ państwa trzeciego wystąpi o przekazanie danych do celów dochodzenia, którego celem jest zwalczanie terroryzmu, samo istnienie przepisów prawa Unii lub państwa członkowskiego, których celem również jest zwalczanie terroryzmu, nie jest wystarczającym powodem do zastosowania art. 49 ust. 1 lit. d) w odniesieniu do takiego przekazania. Raczej, jak podkreśliła Grupa Robocza Art. 29, czyli podmiot poprzedzający Europejską Radę Ochrony Danych, w poprzednich stanowiskach[29], wyjątek ten ma zastosowanie jedynie w przypadku, gdy z prawa Unii lub państwa członkowskiego, któremu podlega administrator, można wywnioskować, że takie przekazanie danych jest dozwolone do ważnych celów interesu publicznego, w tym w duchu wzajemności na rzecz współpracy międzynarodowej. Istnienie międzynarodowej umowy lub konwencji, w której uznano określony cel i przewidziano współpracę międzynarodową, aby wesprzeć osiągnięcie tego celu, może być wskaźnikiem przy ocenie istnienia interesu publicznego na podstawie art. 49 ust. 1 lit. d), pod warunkiem że UE lub państwa członkowskie są stroną tej umowy lub konwencji.

Chociaż art. 49 ust. 1 lit. d) jest głównie przeznaczony do wykorzystania przez organy publiczne, mogą się powoływać na niego również podmioty prywatne. Wniosek taki jest poparty kilkoma przykładami wymienionymi w motywie 112, w którym wspomniano o przekazaniach zarówno przez organy publiczne, jak i podmioty prywatne[30].

W związku z tym zasadniczym wymogiem warunkującym zastosowanie tego wyjątku jest ustalenie istnienia ważnego interesu publicznego, a nie charakter organizacji (organizacja publiczna, prywatna czy międzynarodowa), która przekazuje lub otrzymuje dane.

W motywach 111 i 112 wskazano, że wyjątek ten nie ogranicza się do przekazań danych, które są „sporadyczne"[31]. Nie oznacza to jednak, że przekazania danych na podstawie wyjątku z uwagi na ważny interes publiczny na mocy art. 49 ust. 1 lit. d) mogą następować na dużą skalę i w sposób systematyczny. Należy raczej przestrzegać ogólnej zasady, zgodnie z którą wyjątki określone w art. 49 nie stają się „zasadą" w praktyce, ale należy je ograniczyć do szczególnych sytuacji i każdy podmiot przekazujący dane musi zapewnić, aby przekazanie spełniało rygorystyczne kryterium niezbędności[32].

W przypadku gdy przekazania następują w toku zwykłej działalności lub praktyki, Europejska Rada Ochrony Danych stanowczo zachęca wszystkie podmioty przekazujące dane (w szczególności organy publiczne[33]) do uregulowania przekazań przez wprowadzenie odpowiednich zabezpieczeń zgodnie z art. 46, a nie przez opieranie się na wyjątku określonym w art. 49 ust. 1 lit. d).

[29] Opinia 10/2006 Grupy Roboczej Art. 29 w sprawie przetwarzania danych osobowych przez Stowarzyszenie Międzynarodowej Teletransmisji Danych Finansowych (SWIFT) (WP 128), s. 25.
[30] *„Międzynarodowa wymiana danych między organami ds. konkurencji, organami podatkowymi lub celnymi, organami nadzoru finansowego, służbami odpowiedzialnymi za sprawy zabezpieczenia społecznego lub za zdrowie publiczne, na przykład w przypadku ustalania kontaktów zakaźnych w razie chorób zakaźnych lub w celu zmniejszenia lub wyeliminowania dopingu w sporcie"*.
[31] W odniesieniu do ogólnej definicji terminu „sporadyczne" zob. s. 4.
[32] Zob. również s. 3.
[33] Na przykład organy nadzoru finansowego wymieniające dane w kontekście międzynarodowego przekazywania danych osobowych do celów współpracy administracyjnej.

2.5 Przekazanie jest niezbędne do ustalenia, dochodzenia lub ochrony roszczeń (art. 49 ust. 1 lit. e))

Ustalenie, dochodzenie lub ochrona roszczeń

Zgodnie z art. 49 ust. 1 lit. e) przekazanie może nastąpić, jeśli *„jest niezbędne do ustalenia, dochodzenia lub ochrony roszczeń"*. Motyw 111 stanowi, że przekazanie jest możliwe, jeśli jest *„sporadyczne i niezbędne w związku z umową lub roszczeniem – niezależnie od rodzaju postępowania: sądowego lub administracyjnego lub jakiegokolwiek innego postępowania pozasądowego, w tym postępowania przed organami regulacyjnymi"*. Obejmuje to szereg działań na przykład w kontekście postępowania karnego lub administracyjnego w państwie trzecim (np. prawo dotyczące naruszenia konkurencji, korupcja, wykorzystywanie informacji wewnętrznych lub podobne sytuacje), w przypadku którego wyjątek może mieć zastosowanie do przekazania danych do celów obrony własnej lub uzyskania zmniejszenia przewidzianej w prawie kary pieniężnej lub zwolnienia z niej, np. w postępowaniu w sprawie naruszenia konkurencji. Przekazania danych do celów formalnego, przygotowawczego postępowania ujawniającego w procesie cywilnym mogą również wchodzić w zakres tego wyjątku. Wyjątek ten może również obejmować działania podmiotu przekazującego dane, mające na celu wszczęcie postępowania w państwie trzecim, na przykład w przypadku powództwa sądowego czy ubiegania się o zatwierdzenie połączenia. Wyjątku nie można zastosować, aby uzasadnić przekazanie danych osobowych ze względu na samą możliwość, że postępowanie sądowe lub procedura formalna mogą zostać wszczęte w przyszłości.

Wyjątek ten można stosować do działalności prowadzonej przez organy publiczne w ramach wykonywania przysługujących im uprawnień publicznych (art. 49 ust. 3).

Połączenie terminów „roszczenie" i „postępowanie" oznacza, że odnośne postępowanie musi posiadać podstawę prawną, w tym formalną, określoną w prawie procedurę, jednak niekoniecznie ogranicza się do postępowania sądowego czy administracyjnego („lub jakiegokolwiek innego postępowania pozasądowego"). Ponieważ przekazanie musi się odbyć **w toku** postępowania, konieczne jest ścisłe powiązanie między przekazaniem danych a konkretnym postępowaniem dotyczącym danej sytuacji. Abstrakcyjne zastosowanie określonego rodzaju postępowania nie byłoby wystarczające.

Administratorzy danych i podmioty przetwarzające muszą być świadomi tego, że prawo krajowe również może zawierać tak zwane „ustawy blokujące", zakazujące im przekazywania danych osobowych sądom zagranicznym lub potencjalnie innym zagranicznym organom urzędowym lub ograniczające takie przekazywanie.

Niezbędność przekazania danych

Przekazanie danych może nastąpić wyłącznie wówczas, gdy jest **niezbędne** do ustalenia, dochodzenia lub ochrony danego roszczenia. *„Kryterium niezbędności"* wymaga ścisłego i znacznego powiązania między danymi, które mają być przekazane, a ustaleniem, dochodzeniem lub ochroną sytuacji prawnej[34]. Sam interes organów państwa trzeciego lub potencjalna „dobra wola", którą można uzyskać od organu państwa trzeciego, nie byłyby wystarczające.

Chociaż podmiot przekazujący dane może mieć pokusę, aby przekazać wszystkie potencjalnie istotne dane osobowe w odpowiedzi na wniosek lub do celów wszczęcia postępowania sądowego, nie byłoby to zgodne z tym wyjątkiem lub, ogólniej mówiąc, z RODO, ponieważ (zgodnie z zasadą minimalizacji danych) podkreśla to konieczność, aby dane osobowe były odpowiednie, istotne i ograniczały się do tego, co jest niezbędne w związku z celami, w jakich się je przetwarza.

W odniesieniu do postępowania sądowego Grupa Robocza Art. 29, czyli podmiot poprzedzający Europejską Radę Ochrony Danych, wypracowała już wielopłaszczyznowe podejście do kwestii tego, czy dane osobowe należy przekazywać, w tym do stosowania tej zasady. Na pierwszym etapie należy starannie ocenić, czy dane zanonimizowane nie byłyby wystarczające w danym przypadku. Jeśli nie, wówczas można rozważyć przekazanie danych opatrzonych pseudonimem. Jeżeli przesłanie danych osobowych do państwa trzeciego jest konieczne, ich istotność dla danej sprawy należy ocenić przed przekazaniem – tak aby przekazany i ujawniony został jedynie zbiór tych danych osobowych, które są faktycznie niezbędne.

Sporadyczne przekazanie

Przekazania takie powinny następować tylko wtedy, gdy są sporadyczne. Aby zapoznać się z informacjami na temat definicji przekazań sporadycznych, zob. odpowiednia sekcja dotycząca „sporadycznych" i „niepowtarzających się" przekazań[35]. Podmioty przekazujące dane musiałyby staranie ocenić każdy przypadek z osobna.

2.6 Przekazanie niezbędne do ochrony żywotnych interesów osoby, których dane dotyczą, lub innych osób, jeżeli osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody (art. 49 ust. 1 lit. f))

Wyjątek przewidziany w art. 49 ust. 1 lit. f) ma oczywiście zastosowanie, w przypadku gdy dane przekazywane są w sytuacji zagrożenia zdrowia, jeżeli uznaje się, że takie przekazanie jest niezbędne w celu zapewnienia niezbędnej opieki medycznej.

W związku z tym zgodnie z prawem możliwe musi być na przykład przekazanie danych (w tym pewnych danych osobowych), jeżeli osoba, której dane dotyczą, podczas przebywania poza granicami UE jest nieprzytomna i wymaga natychmiastowej opieki medycznej, a jedynie podmiot przekazujący dane (tj. lekarz tej osoby), prowadzący praktykę w państwie członkowskim UE, jest w stanie dostarczyć takie dane. W takich przypadkach prawo przewiduje, że ryzyko doznania poważnej szkody przez osobę, której dane dotyczą, przeważa nad aspektami ochrony danych.

Przekazanie musi być związane z interesem osoby, której dane dotyczą, lub interesem innej osoby, a także jeżeli przekazywane dane dotyczą zdrowia, ich przekazanie musi być konieczne w celu postawienia koniecznej diagnozy. Podobnie wyjątku tego nie można zastosować w celu uzasadnienia przekazywania osobistych danych medycznych poza UE, jeżeli celem przekazania nie jest leczenie szczególnego przypadku osoby, której dane dotyczą, lub innej osoby, ale na przykład przeprowadzenie ogólnego badania medycznego, którego wyniki będą dostępne w przyszłości.

W RODO rzeczywiście nie ograniczono stosowania tego wyjątku w odniesieniu do integralności fizycznej osoby, ale pozostawiono na przykład możliwość rozważenia przypadków, w których należy chronić integralność psychiczną osoby. W takim przypadku dana osoba również byłaby niezdolna – fizycznie lub prawnie – do wyrażenia zgody na przekazanie swoich danych osobowych. Ponadto zainteresowana osoba fizyczna, której dane osobowe są przedmiotem przekazania, musi w szczególności nie być w stanie – fizycznie lub prawnie – udzielić zgody na to przekazanie.

Jeżeli jednak osoba, której dane dotyczą, jest w stanie podjąć ważną decyzję i istnieje możliwość ubiegania się o jej zgodę, nie można zastosować tego wyjątku.

[34] Motyw 111: „niezbędne w związku z umową lub roszczeniem".

[35] S. 4.

Na przykład gdy dane osobowe są konieczne, aby zapobiec eksmisji z nieruchomości, sytuacja ta nie wchodzi w zakres tego wyjątku, ponieważ mimo iż zakwaterowanie można uznać za żywotny interes, osoba, której dane dotyczą, może wyrazić zgodę na przekazanie swoich danych.

Ta zdolność do podjęcia ważnej decyzji może zależeć od niezdolności fizycznej, psychicznej, ale również prawnej. Niezdolność prawna może na przykład obejmować, bez uszczerbku dla krajowych mechanizmów reprezentacji, przypadek małoletniego. Taką niezdolność prawną należy udowodnić, w zależności od przypadku, na podstawie orzeczenia lekarskiego poświadczającego psychiczną niezdolność osoby, której dane dotyczą, albo na podstawie dokumentu rządowego potwierdzającego sytuację prawną danej osoby.

Przekazanie do międzynarodowej organizacji humanitarnej danych, które są niezbędne, aby wykonać zobowiązanie wynikające z konwencji genewskich lub aby działać zgodnie z międzynarodowym prawem humanitarnym obowiązującym podczas konfliktu zbrojnego, również może wchodzić w zakres art. 49 ust. 1 lit. f); zob. motyw 112. W takich przypadkach osoba, której dane dotyczą, również musi być fizycznie lub prawnie niezdolna do wyrażenia zgody.

Przekazanie danych osobowych po wystąpieniu katastrofy naturalnej i w kontekście udostępniania danych osobowych podmiotom i osobom w celu przeprowadzenia działań ratowniczych i poszukiwawczych (na przykład krewnym ofiar katastrofy, a także rządowi i służbom ratunkowym) można uzasadnić na podstawie tego wyjątku. Takie nieoczekiwane zdarzenia (powodzie, trzęsienia ziemi, huragany itd.) mogą uzasadniać pilne przekazanie pewnych danych osobowych, aby poznać na przykład miejsce, w którym znajdują się ofiary, oraz ich stan. W takich sytuacjach uznaje się, że osoba, której dane dotyczą, nie jest w stanie wyrazić zgody na przekazanie swoich danych.

2.7 Przekazanie danych z publicznego rejestru (art. 49 ust. 1 lit. g) i art. 49 ust. 2)

W art. 49 ust. 1 lit. g) i art. 49 ust. 2 zezwolono na przekazanie danych osobowych z rejestrów pod pewnymi warunkami. Rejestr definiuje się zwykle jako *„(pisemny) spis zawierający regularnie dokonywane wpisy dotyczące rzeczy lub szczegóły”* lub jako „oficjalny wykaz lub spis nazw lub rzeczy”[36], przy czym w kontekście art. 49 rejestr może mieć formę pisemną lub elektroniczną.

Zgodnie z prawem Unii lub prawem państwa członkowskiego rejestr taki ma służyć za źródło informacji dla ogółu obywateli. W związku z tym prywatne rejestry (za które odpowiadają podmioty prywatne) wykraczają poza zakres tego wyjątku (na przykład prywatne rejestry, na których podstawie ocenia się zdolność kredytową).

Rejestr musi być dostępny dla:

a) ogółu obywateli lub

b) dla każdej osoby mogącej wykazać prawnie uzasadniony interes.

Mogą to być na przykład: rejestry przedsiębiorstw, rejestry stowarzyszeń, rejestry wyroków skazujących, rejestry tytułów własności (gruntów) lub publiczne rejestry pojazdów.

Poza ogólnymi wymogami dotyczącymi ustanowienia samych rejestrów przekazanie danych z tych rejestrów można nastąpić wyłącznie wówczas, gdy w każdym szczególnym przypadku spełniono warunki konsultacji określone w prawie Unii lub prawie państwa członkowskiego (informacje na temat tych ogólnych warunków można znaleźć w art. 49 ust. 1 lit. g)).

[36] Merriam Webster Dictionary, https://www.merriam-webster.com/dictionary/register (22.01.2018); Oxford Dictionary https://en.oxforddictionaries.com/definition/register (22.01.2018).

Administratorzy danych i podmioty przetwarzające chcące przekazać dane osobowe na mocy tego wyjątku muszą zdawać sobie sprawę, że przekazanie nie może obejmować całości danych osobowych ani całych kategorii danych osobowych zawartych w rejestrze (art. 49 ust. 2). Jeżeli przekazanie następuje z rejestru utworzonego na mocy prawa i przeznaczonego do wglądu dla ogółu obywateli lub osób mających prawnie uzasadniony interes, przekazanie danych może nastąpić wyłącznie na żądanie tych osób lub jeżeli osoby te są odbiorcami, przy uwzględnieniu interesów i praw podstawowych osób, których dane dotyczą[37]. Przy ocenie, czy przekazanie jest właściwe w danym przypadku, podmioty przekazujące dane zawsze będą musiały wziąć pod uwagę interesy i prawa osoby, której dane dotyczą.

Dalsze przetwarzanie danych osobowych pochodzących z takich rejestrów, jak określono powyżej, można przeprowadzić wyłącznie zgodnie z obowiązującymi przepisami o ochronie danych.

Wyjątek ten można stosować również do działalności prowadzonej przez organy publiczne w ramach wykonywania przysługujących im uprawnień publicznych (art. 49 ust. 3).

2.8 Ważne prawnie uzasadnione interesy (art. 49 ust. 1 akapit drugi)

W art. 49 ust. 1 akapit drugi wprowadzono nowy wyjątek, którego nie zawierała wcześniej dyrektywa. Na podstawie szeregu konkretnych, wyraźnie wymienionych warunków dane osobowe można przekazać, jeżeli jest to niezbędne ze względu na ważne prawnie uzasadnione interesy realizowane przez podmiot przekazujący dane.

Wyjątek ten przewidziano w prawie jako ostateczne rozwiązanie, ponieważ będzie on miał zastosowanie wyłącznie w przypadku, gdy *„przekazanie nie może się opierać na art. 45 ani 46, w tym na przepisach dotyczących wiążących reguł korporacyjnych, i nie ma zastosowania żaden z wyjątków mających zastosowanie w szczególnych sytuacjach”*[38].

To wielopłaszczyznowe podejście do rozważania stosowania wyjątków jako podstaw przekazywania wymaga sprawdzenia, czy możliwe jest zastosowanie narzędzia przekazywania określonego w art. 45 lub 46 lub jednego ze szczególnych wyjątków określonych w art. 49 ust. 1 akapit pierwszy, przed powołaniem się na wyjątek określony w art. 49 ust. 1 akapit drugi. Można go zastosować jedynie w nielicznych przypadkach, jak określono w motywie 113, i jest on zależny od znacznej liczby warunków wyraźnie przewidzianych przepisami prawa. Zgodnie z zasadą rozliczalności zapisaną w RODO[39] podmiot przekazujący dane musi być w stanie wykazać, że przekazanie danych z zastosowaniem odpowiednich zabezpieczeń na podstawie art. 46 ani zastosowanie jednego z wyjątków przedstawionych w art. 49 ust. 1 akapit pierwszy nie było możliwe.

Sugeruje to, że podmiot przekazujący dane podjął poważne próby w tym zakresie, uwzględniając okoliczności przekazania danych. Może to na przykład, w zależności od przypadku, obejmować wykazanie przeprowadzenia weryfikacji, czy przekazanie danych może nastąpić na podstawie wyraźnej zgody na przekazanie udzielonej przez osobę, której dane dotyczą, zgodnie z art. 49 ust. 1 lit. a). W pewnych okolicznościach zastosowanie innych narzędzi może jednak być praktycznie niemożliwe. Na przykład niektóre rodzaje odpowiednich zabezpieczeń na podstawie art. 46 mogą nie być w praktyce opcją dostępną dla podmiotu przekazującego dane będącego małym lub średnim przedsiębiorstwem[40]. Może się tak zdarzyć na przykład również wówczas, gdy podmiot odbierający dane wyraźnie odmówił zawarcia umowy w sprawie przekazania danych na podstawie standardowych

[37] Motyw 111 RODO.
[38] Art. 49 ust. 1 akapit drugi RODO.
[39] Art. 5 ust. 2 i art. 24 ust. 1.
[40] Często na przykład wiążące reguły korporacyjne mogą nie być wykonalną opcją dla małych lub średnich przedsiębiorstw, ponieważ wiążą się ze znacznymi inwestycjami administracyjnymi.

klauzul ochrony danych (art. 46 ust. 2 lit. c)), a żadna z pozostałych możliwości nie jest dostępna (w tym, w zależności od przypadku, wybór innego „podmiotu odbierającego dane") – zob. również pkt poniżej dotyczący „ważnych" prawnie uzasadnionych interesów.

Ważne prawnie uzasadnione interesy administratora danych

Zgodnie z brzmieniem wyjątku przekazanie musi być niezbędne do celów realizacji ważnych prawnie uzasadnionych interesów administratora danych, nad którymi nie przeważają interesy lub prawa i wolności osoby, której dane dotyczą. Uwzględnienie interesów podmiotu przekazującego dane działającego jako podmiot przetwarzający lub podmiotu odbierającego dane nie jest istotne.

Ponadto istotne są wyłącznie interesy, które można uznać za „ważne", co ogranicza w znacznym stopniu zakres stosowania wyjątku, ponieważ nie wszystkie możliwe „prawnie uzasadnione interesy" na mocy art. 6 ust. 1 lit. f) będą miały zastosowanie w tym przypadku. Zastosowanie będzie mieć raczej pewien wyższy próg, zgodnie z którym ważne prawnie uzasadnione interesy będą musiały być kluczowe dla administratora danych. Przykładem może być sytuacja, w której administrator danych jest zmuszony przekazać dane osobowe, aby chronić swoją organizację lub systemy przed poważną bezpośrednią szkodą lub przed dotkliwą karą, które miałyby poważny wpływ na jego działalność gospodarczą.

Niepowtarzające się przekazanie

Jak wyraźnie wskazano w art. 49 ust. 1 akapit drugi, przepis ten ma zastosowanie wyłącznie do przekazania, które nie jest powtarzalne[41].

Ograniczona liczba osób, których dane dotyczą

Przekazanie danych musi również dotyczyć tylko ograniczonej liczby osób, których dane dotyczą. Nie ustalono żadnego bezwzględnego progu, ponieważ będzie on zależny od kontekstu, ale liczba ta musi być odpowiednio mała, biorąc pod uwagę rodzaj odnośnego przekazania.

W praktyce pojęcie „ograniczona liczba osób, których dane dotyczą" zależy od konkretnego przypadku. Na przykład jeżeli administrator danych musi przekazać dane osobowe, aby wykryć wyjątkowy i poważny incydent bezpieczeństwa w celu ochrony swojej organizacji, trzeba będzie rozstrzygnąć, dane ilu pracowników administrator musiałby przekazać, aby zrealizować ten ważny prawnie uzasadniony interes.

W takiej sytuacji, aby można było zastosować wyjątek, przekazanie takie nie powinno dotyczyć wszystkich pracowników administratora danych, ale raczej pewnej ograniczonej ich liczby.

Wyważenie „ważnych prawnie uzasadnionych interesów administratora" i „interesów lub praw i wolności osoby, której dane dotyczą" na podstawie oceny wszystkich okoliczności towarzyszących przekazaniu danych i zapewnienie odpowiednich zabezpieczeń

Zgodnie z kolejnym wymogiem należy przeprowadzić test polegający na wyważeniu (ważnego) prawnie uzasadnionego interesu realizowanego przez podmiot przekazujący dane i interesów lub praw i wolności osoby, której dane dotyczą. W tym zakresie prawo wyraźnie wymaga, aby podmiot przekazujący dane przeprowadził ocenę wszystkich okoliczności towarzyszących przedmiotowemu przekazaniu danych i zapewnił na podstawie tej oceny odpowiednie zabezpieczenia w celu ochrony przekazywanych danych. Wymóg ten stanowi podkreślenie szczególnej roli, jaką mogą odgrywać zabezpieczenia pod względem zmniejszenia nadmiernego wpływu przekazania danych na osoby, których dane dotyczą, a tym samym możliwego wpływu na równowagę praw i interesów w takim stopniu, że interesy administratora danych nie będą podrzędne[42].

Jeżeli chodzi o interesy, prawa i wolności osoby, której dane dotyczą, które należy wziąć pod uwagę, należy uważnie przewidzieć i ocenić możliwe negatywne skutki, tj. ryzyko wiążące się z przekazaniem danych w odniesieniu do jakiegokolwiek (uzasadnionego) interesu osoby, której dane dotyczą, biorąc pod uwagę prawdopodobieństwo i wagę ryzyka[43]. W tym zakresie należy wziąć pod uwagę w szczególności wszelkie możliwe szkody (fizyczne i majątkowe, ale również niemajątkowe, np. dotyczące utraty reputacji)[44]. Podczas oceny tych zagrożeń i środków, które można by w takich okolicznościach uznać za „odpowiednie zabezpieczenia" praw i wolności osoby, której dane dotyczą, podmiot przekazujący dane musi uwzględnić w szczególności charakter danych, cel i czas trwania przetwarzania, a także sytuację w państwie pochodzenia, państwie trzecim i w ewentualnym państwie ostatecznego przeznaczenia przekazania[45].

Ponadto prawo wymaga, aby podmiot przekazujący dane stosował dodatkowe środki jako zabezpieczenia w celu ograniczenia zidentyfikowanego ryzyka dla osoby, której dane dotyczą, wynikającego z przekazania danych[46]. W prawie określono to działanie jako obowiązkowy wymóg, można zatem uznać, że w razie braku dodatkowych zabezpieczeń interesy administratora danych związane z przekazaniem będą w każdym przypadku podrzędne wobec interesów lub praw i wolności osoby, której dane dotyczą[47]. Jeżeli chodzi o charakter zabezpieczeń, ustanowienie ogólnych wymogów mających zastosowanie do wszystkich przypadków w tym zakresie nie jest możliwe, będzie on raczej zależeć w znacznym stopniu od danego szczególnego przekazania danych. Zabezpieczenia mogą obejmować, w zależności od przypadku, na przykład środki mające na celu zapewnienie jak najszybszego usunięcia danych po przekazaniu lub środki ograniczające cele przetwarzania danych po ich przekazaniu. Szczególny nacisk należy położyć na sprawdzenie, czy zabezpieczenie jest wystarczające, aby przekazać dane opatrzone pseudonimem lub zaszyfrowane[48]. Ponadto należy zbadać środki techniczne i organizacyjne mające na celu zapewnienie, by przekazane dane nie zostały wykorzystane w innych celach niż cele ściśle przewidziane przez podmiot przekazujący dane.

[41] Więcej informacji na temat wyrażenia „nie jest powtarzalne" można znaleźć na s. 4.

[42] Ważną rolę zabezpieczeń w kontekście wyważenia interesów administratora danych i osób, których dane dotyczą, podkreśliła już Grupa Robocza Art. 29 w dokumencie WP 217, s. 31.

[43] Zob. motyw 75: *„Ryzyko naruszenia praw lub wolności osób, o różnym prawdopodobieństwie i wadze zagrożeń (...)"*.

[44] Zob. motyw 75: *„Ryzyko naruszenia praw lub wolności osób, o różnym prawdopodobieństwie i wadze zagrożeń, może wynikać z przetwarzania danych osobowych mogącego prowadzić do uszczerbku fizycznego lub szkód majątkowych lub niemajątkowych"*.

[45] Motyw 113.

[46] Chociaż w kontekście „zwykłego" przewidzianego w prawie testu polegającego na wyważeniu interesów takie (dodatkowe) środki mogą nie być konieczne w każdym przypadku (zob. dokument roboczy Grupy Roboczej Art. 29 w sprawie projektu klauzul umownych *ad hoc* dotyczących przekazywania danych przez przetwarzającego w UE do podprzetwarzającego spoza UE (WP 214), s. 41), brzmienie art. 49 ust. 1 akapit drugi sugeruje, że dodatkowe środki są obowiązkowe, aby przekazanie danych było zgodne z „testem polegającym na wyważeniu interesów", a zatem wykonalne na mocy tego wyjątku.

[47] Chociaż w kontekście „zwykłego" przewidzianego w prawie testu polegającego na wyważeniu interesów takie (dodatkowe) środki mogą nie być konieczne w każdym przypadku (zob. Opinia 6/2014 Grupy Roboczej Art. 29 w sprawie pojęcia prawnie uzasadnionych interesów administratora danych na mocy artykułu 7 dyrektywy 95/46/WE (WP 217), s. 41), brzmienie art. 49 ust. 1 akapit drugi sugeruje, że dodatkowe środki są obowiązkowe, aby przekazanie danych było zgodne z „testem polegającym na wyważeniu interesów", a zatem wykonalne na mocy tego wyjątku.

[48] Inne przykłady możliwych zabezpieczeń można znaleźć w dokumencie roboczym Grupy Roboczej Art. 29 w sprawie projektu klauzul umownych *ad hoc* dotyczących przekazywania danych przez przetwarzającego w UE do podprzetwarzającego spoza UE (WP 214), s. 41–43.

Udzielenie informacji organowi nadzorczemu

Obowiązek udzielenia informacji organowi nadzorczemu nie oznacza, że organ nadzorczy musi zatwierdzić przekazanie danych, ale stanowi raczej dodatkowe zabezpieczenie, ponieważ umożliwia organowi nadzorczemu ocenę możliwego wpływu przekazania danych (jeżeli organ uzna przekazanie za odpowiednie) na prawa i wolności osób, których dane dotyczą. W ramach działania zgodnie z zasadą rozliczalności zaleca się, aby podmiot przekazujący dane zapisywał wszystkie istotne aspekty przekazania danych, np. realizowane ważne prawnie uzasadnione interesy, „ważne" interesy osób fizycznych, charakter przekazywanych danych i cel przekazania danych.

Podanie osobie, której dane dotyczą, informacji na temat przekazania danych i realizowanych ważnych prawnie uzasadnionych interesów

Administrator danych musi podać osobie, której dane dotyczą, informacje na temat przekazania danych i realizowanych ważnych prawnie uzasadnionych interesów. Informacje te należy przekazać wraz z informacjami, których podanie jest wymagane na mocy art. 13 i 14 RODO.

W imieniu Europejskiej Rady Ochrony Danych,

Przewodnicząca

(Andrea Jelinek)



Wytyczne 1/2018 w sprawie certyfikacji i określenia kryteriów certyfikacji zgodnie z art. 42 i 43 rozporządzenia

Wersja 3.0

4 czerwca 2019 r.

Translations proofread by EDPB Members.
This language version has not yet been proofread.

Tekst przyjęty

Historia wersji

Wersja 3.0	4 czerwca 2019 r.	Włączenie załącznika 2 (wersja 2.0 załącznika 2 przyjęta w dniu 4 czerwca 2019 r. po konsultacjach publicznych)
Wersja 2.1	9 kwietnia 2019 r.	Przyjęcie sprostowania do wytycznych (pkt 45)
Wersja 2.0	23 stycznia 2019 r.	Przyjęcie wytycznych po przeprowadzeniu konsultacji publicznych – W tym samym dniu załącznik 2 (wersja 1.0) został przyjęty do konsultacji publicznych.
Wersja 1.0	25 maja 2018 r.	Przyjęcie wytycznych do konsultacji w sprawie publikacji

Spis treści

1 Wprowadzenie 5
1.1 Zakres wytycznych 6
1.2 Cel certyfikacji na podstawie RODO 7
1.3 Kluczowe pojęcia 8
1.3.1 Interpretacja „certyfikacji” 8
1.3.2 Mechanizmy certyfikacji, znaki jakości i oznaczenia 9
2 Rola organów nadzorczych 9
2.1 Organ nadzorczy jako podmiot certyfikujący 10
2.2 Dalsze zadania organu nadzorczego w odniesieniu do certyfikacji 10
3 Rola podmiotu certyfikującego 11
4 Zatwierdzenie kryteriów certyfikacji 12
4.1 Zatwierdzenie kryteriów przez właściwy organ nadzorczy 12
4.2 Zatwierdzanie przez EROD kryteriów dotyczących europejskiego znaku jakości ochrony danych 13
4.2.1 Wniosek o zatwierdzenie 13
4.2.2 Kryteria dotyczące europejskiego znaku jakości ochrony danych 14
4.2.3 Rola akredytacji 15
5 Opracowywanie kryteriów certyfikacji 15
5.1 Co może być przedmiotem certyfikacji na podstawie RODO? 16
5.2 Określenie przedmiotu certyfikacji 17
5.3 Metody ewaluacji i metodyka oceny 19
5.4 Dokumentacja oceny 20
5.5 Dokumentacja wyników 20
6 Wytyczne dotyczące określania kryteriów certyfikacji 21
6.1 Istniejące normy 22
6.2 Określenie kryteriów 22
6.3 Okres ważności kryteriów certyfikacji 23
Załącznik 1: Zadania i uprawnienia organów nadzorczych w odniesieniu do certyfikacji na podstawie RODO 24
Załącznik 2 25
1 Wprowadzenie 25
2 Zakres mechanizmu certyfikacji i przedmiot oceny 25
3 Wymogi ogólne 26
4 Operacja przetwarzania, art. 42 ust. 1 27

5 Zgodność przetwarzania z prawem 27
6 Zasady, art. 5 27
7 Ogólne obowiązki administratorów i podmiotów przetwarzających 27
8 Prawa osób, których dane dotyczą 28
9 Ryzyko naruszenia praw lub wolności osób fizycznych 28
10 Środki techniczne i organizacyjne gwarantujące ochronę 28
11 Inne cechy szczególne sprzyjające ochronie danych 29
12 Kryteria służące wykazaniu istnienia odpowiednich zabezpieczeń w odniesieniu do przekazywania danych osobowych 30
13 Dodatkowe kryteria dotyczące europejskiego znaku jakości ochrony danych 30
14 Ogólna ocena kryteriów 30

Europejska Rada Ochrony Danych,

uwzględniając art. 70 ust. 1 lit. e) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (zwanego dalej „RODO"),

uwzględniając Porozumienie EOG, w szczególności załącznik XI i protokół 37 do tego Porozumienia, zmienione decyzją Wspólnego Komitetu EOG nr 154/2018 z dnia 6 lipca 2018 r.,

uwzględniając art. 12 i 22 swojego regulaminu wewnętrznego z dnia 25 maja 2018 r.,

biorąc pod uwagę wyniki konsultacji publicznych w sprawie wytycznych, które odbyły się w dniach 30 maja 2018 r. – 12 lipca 2018 r., oraz w sprawie załącznika 2, które odbyły się w dniach 15 lutego – 29 marca 2019 r., zgodnie z art. 70 ust. 4 RODO,

PRZYJĘŁA NASTĘPUJĄCE WYTYCZNE:

1 WPROWADZENIE

1. W ogólnym rozporządzeniu o ochronie danych (rozporządzenie 2016/279, „RODO" lub „rozporządzenie") przedstawiono zmodernizowane ramy zgodności z przepisami dotyczącymi rozliczalności i praw podstawowych do celów ochrony danych w Europie. Kluczowe znaczenie w tych nowych ramach ma szereg środków, które ułatwiają przestrzeganie przepisów RODO. Środki te obejmują obowiązkowe wymogi w określonych okolicznościach (w tym powołanie inspektorów ochrony danych i przeprowadzenie ocen skutków dla ochrony danych) oraz dobrowolne środki takie jak kodeksy postępowania i mechanizmy certyfikacji.
2. Przed przyjęciem RODO Grupa Robocza Art. 29 ustaliła, że certyfikacja może odgrywać istotną rolę w ramach rozliczalności do celów ochrony danych1. Aby za pomocą certyfikacji zapewnić wiarygodne dowody na zgodność z przepisami o ochronie danych, należy wprowadzić jasne zasady określające wymogi dotyczące świadczenia usług certyfikacyjnych2. W art. 42 RODO zapewniono podstawę prawną dotyczącą opracowania takich zasad.
3. Art. 42 ust. 1 RODO stanowi, że:

„Państwa członkowskie, organy nadzorcze, Europejska Rada Ochrony Danych oraz Komisja zachęcają – w szczególności na szczeblu Unii – do ustanawiania mechanizmów certyfikacji oraz znaków jakości i oznaczeń w zakresie ochrony danych osobowych mających świadczyć o zgodności z niniejszym rozporządzeniem operacji przetwarzania prowadzonych przez administratorów i podmioty przetwarzające. Przy tym uwzględnia się szczególne potrzeby mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw".

[1] Grupa Robocza Art. 29, opinia 3/2010 w sprawie zasady rozliczalności, WP173, 13 lipca 2010 r., pkt 69–71.
[2] Grupa Robocza Art. 29, opinia 3/2010 w sprawie zasady rozliczalności, WP173, pkt 69.

4. Mechanizmy certyfikacji3 mogą przyczynić się do poprawy przejrzystości dla osób, których dane dotyczą, a także do poprawy stosunków między przedsiębiorstwami, np. między administratorami i podmiotami przetwarzającymi. W motywie 100 RODO stwierdzono, że ustanowienie mechanizmów certyfikacji może zwiększyć przejrzystość i poprawić przestrzeganie rozporządzenia oraz pozwolić w ten sposób osobom, których dane dotyczą, szybko ocenić stopień ochrony danych, której podlegają stosowne produkty i usługi4.

5. W RODO nie wprowadza się prawa ani obowiązku certyfikacji dla administratorów i podmiotów przetwarzających; zgodnie z art. 42 ust. 3 certyfikacja jest procesem dobrowolnym, który ma pomóc w wykazaniu przestrzegania RODO. Państwa członkowskie oraz organy nadzorcze wzywa się do zachęcania do ustanawiania mechanizmów certyfikacji; określą też one zaangażowanie zainteresowanych stron w proces certyfikacji oraz cykl życia certyfikacji.

6. Ponadto zgodność z zatwierdzonymi mechanizmami certyfikacji jest czynnikiem, który organy nadzorcze muszą brać pod uwagę jako czynnik obciążający lub łagodzący, gdy decydują się na zastosowanie administracyjnej kary pieniężnej oraz kiedy ustalają wysokość tej kary (art. 83 ust. 2 lit. j))5.

1.1 Zakres wytycznych

7. Niniejsze wytyczne mają ograniczony zakres; nie są one podręcznikiem procedur dotyczących certyfikacji zgodnie z RODO. Głównym celem niniejszych wytycznych jest określenie nadrzędnych wymogów i kryteriów, które mogą mieć zastosowanie do wszystkich rodzajów mechanizmów certyfikacji opracowanych zgodnie z art. 42 i 43 RODO. W tym celu w wytycznych:

    - zbadano zasadność certyfikacji jako narzędzia rozliczalności;
    - wyjaśniono kluczowe pojęcia zastosowane w przepisach dotyczących certyfikacji zawartych w art. 42 i 43; a także
    - wyjaśniono zakres możliwych przedmiotów certyfikacji zgodnie z art. 42 i 43 oraz cel certyfikacji;
    - ułatwiono uzyskiwanie miarodajnych, jednoznacznych, możliwie jak najbardziej powtarzalnych i porównywalnych wyników certyfikacji, niezależnie od jednostki certyfikującej (porównywalność).

8. W RODO zezwala się państwom członkowskim i organom nadzorczym na wdrażanie przepisów art. 42 i 43 na wiele sposobów. W wytycznych przedstawiono porady dotyczące interpretacji i wdrażania przepisów art. 42 i 43, co pomoże państwom członkowskim, organom nadzorczym oraz krajowym jednostkom akredytującym w ustanowieniu bardziej spójnego, zharmonizowanego podejścia do wdrażania mechanizmów certyfikacji zgodnie z RODO.

9. Porady zawarte w wytycznych będą istotne dla:

    - właściwych organów nadzorczych oraz dla Europejskiej Rady Ochrony Danych („EROD") przy zatwierdzaniu kryteriów certyfikacji na podstawie art. 42 ust. 5, art. 58 ust. 3 lit. f) oraz art. 70 ust. 1 lit. o);
    - podmiotów certyfikujących przy określaniu i dokonywaniu przeglądu kryteriów certyfikacji przed przedłożeniem ich do zatwierdzenia właściwemu organowi nadzorczemu zgodnie z art. 42 ust. 5;
    - EROD przy zatwierdzaniu europejskiego znaku jakości ochrony danych na podstawie art. 42 ust. 5 i art. 70 ust. 1 lit. o);
    - organów nadzorczych przy opracowywaniu ich własnych kryteriów certyfikacji;
    - Komisji Europejskiej, która jest uprawniona do przyjmowania aktów delegowanych w celu doprecyzowania wymogów uwzględnianych w odniesieniu do mechanizmów certyfikacji na podstawie art. 43 ust. 8;
    - EROD podczas udzielania Komisji Europejskiej opinii w sprawie wymogów certyfikacyjnych zgodnie z art. 70 ust. 1 lit. q) i art. 43 ust. 8;
    - krajowych jednostek akredytujących, które będą musiały brać pod uwagę kryteria certyfikacji z myślą o akredytacji podmiotów certyfikujących zgodnie z normą EN-ISO/IEC 17065/2012, a także dodatkowe wymogi zgodnie z art. 43; a także
    - administratorów i podmiotów przetwarzających przy określaniu ich własnej strategii zapewniania zgodności z RODO oraz rozważaniu certyfikacji jako sposobu wykazywania zgodności z przepisami.

10. EROD opublikuje osobne wytyczne dotyczące kwestii określania kryteriów zatwierdzania mechanizmów certyfikacji jako narzędzi przekazywania do państw trzecich lub organizacji międzynarodowych zgodnie z art. 42 ust. 2.

1.2 Cel certyfikacji na podstawie RODO

11. W art. 42 ust. 1 stwierdzono, że mechanizmy certyfikacji ustanawia się, by świadczyły „o zgodności z niniejszym rozporządzeniem operacji przetwarzania prowadzonych przez administratorów i podmioty przetwarzające".

12. RODO stanowi przykład kontekstu, w którym zatwierdzone mechanizmy certyfikacji można wykorzystywać do wykazania wypełnienia zobowiązań przez administratorów i podmioty przetwarzające, które to zobowiązania dotyczą:

    - wdrażania i wykazywania istnienia odpowiednich środków technicznych i organizacyjnych, o których mowa w art. 24 ust. 1 i 3, art. 25 oraz art. 32 ust. 1 i 3;

[3] Niniejsze wytyczne będą odnosiły się do mechanizmów certyfikacji oraz znaków jakości i oznaczeń w dziedzinie ochrony danych łącznie jako do „mechanizmów certyfikacji", zob. sekcja 1.3.2.
[4] W motywie 100 stwierdzono, że należy zachęcać do ustanowienia mechanizmów certyfikacji, aby zwiększyć przejrzystość i poprawić przestrzeganie rozporządzenia, pozwalając w ten sposób osobom, których dane dotyczą, szybko ocenić stopień ochrony danych, której podlegają stosowne produkty i usługi.
[5] Zob. Grupa Robocza Art. 29, Wytyczne w sprawie stosowania i ustalania administracyjnych kar pieniężnych do celów rozporządzenia 2016/679, (WP 253).

- wystarczających gwarancji (ze strony podmiotu przetwarzającego względem administratora), o których mowa w art. 28 ust. 5 akapit 1 oraz (ze strony jednego podmiotu przetwarzającego względem innego podmiotu przetwarzającego) w art. 28 ust. 5 akapit 4.

13. Ponieważ za pomocą certyfikacji samej w sobie nie można udowodnić zgodności z przepisami, a stanowi ona raczej element, który można wykorzystać w celu wykazania zgodności, należy jej dokonywać w sposób przejrzysty. Wykazanie zgodności wymaga posiadania dokumentów potwierdzających, specjalnie w tym celu sporządzonych sprawozdań, w których nie tylko zostaną powtórzone kryteria, ale będzie też opisane, w jaki sposób są one spełniane, oraz – jeżeli nie były spełniane od początku – jakie korekty i działania naprawcze wprowadzono, jak również stosowność takich korekt i działań; tym samym zostaną przedstawione powody przyznania i utrzymania certyfikacji. Powyższe obejmuje zarys indywidualnej decyzji dotyczącej udzielenia, przedłużenia lub cofnięcia certyfikatu. W dokumentach tych powinny znaleźć się powody, argumenty i dowody wynikające z zastosowania kryteriów oraz konkluzje, sądy lub wnioski sformułowane na podstawie faktów lub przesłanek zgromadzonych podczas certyfikacji.

1.3 Kluczowe pojęcia

14. W niniejszej sekcji przeanalizowano kluczowe pojęcia zawarte w art. 42 i 43. W analizie tej rozwinięto rozumienie podstawowych terminów oraz zakresu certyfikacji na podstawie RODO.

1.3.1 Interpretacja „certyfikacji"

15. W RODO nie zdefiniowano terminu „certyfikacja". Międzynarodowa Organizacja Normalizacyjna (ISO) przedstawia uniwersalną definicję pojęcia certyfikacji jako „dostarczenia przez niezależny organ pisemnego zapewnienia (certyfikatu), że dany produkt, usługa lub system spełnia określone wymagania". Certyfikacja jest również nazywana „oceną zgodności przez stronę trzecią", a podmioty certyfikujące mogą być również nazywane „jednostkami oceniającymi zgodność". W normie EN-ISO/IEC 17000:2004 – Ocena zgodności – Słownictwo i ogólne zasady (do których odwołuje się norma ISO17065) – certyfikację definiuje się w następujący sposób: „Zaświadczenie przez osobę trzecią (...) związane z produktami, procesami i usługami".

16. Zaświadczenie jest „kwestią oświadczenia na podstawie podjętej po przeglądzie decyzji, że wykazano spełnienie określonych wymagań" (rozdział 5.2, ISO 17000: 2004).

17. W kontekście certyfikacji na podstawie art. 42 i 43 RODO certyfikacja dotyczy zaświadczenia osoby trzeciej odnoszącego się do operacji przetwarzania dokonywanych przez administratorów i podmioty przetwarzające.

1.3.2 Mechanizmy certyfikacji, znaki jakości i oznaczenia

18. W RODO nie zdefiniowano „mechanizmów certyfikacji, znaków jakości i oznaczeń", a terminy te stosuje się łącznie. Certyfikat jest oświadczeniem o zgodności. Znak jakości lub oznaczenie można wykorzystać w celu potwierdzenia pomyślnego zakończenia procedury certyfikacji. Znak jakości lub oznaczenie najczęściej odnosi się do logo lub symbolu, których obecność (poza certyfikatem) świadczy o tym, że przedmiot certyfikacji poddano niezależnej ocenie oraz że spełnia on dane wymogi określone w dokumentach normatywnych, takich jak przepisy, normy lub specyfikacje techniczne. Wymogi te w kontekście certyfikacji na podstawie RODO określono w dodatkowych wymaganiach, które stanowią uzupełnienie zasad akredytacji podmiotów certyfikujących zawartych w normie EN-ISO/IEC 17065/2012 oraz kryteriów certyfikacji zatwierdzonych przez właściwy organ nadzorczy lub EROD. Certyfikat, znak jakości lub oznaczenie na podstawie RODO mogą zostać przyznane wyłącznie po przeprowadzeniu przez akredytowany podmiot certyfikujący lub właściwy organ nadzorczy niezależnej oceny dowodów, w której zostanie stwierdzone, że spełniono kryteria certyfikacji.

19. W tabeli przedstawiono ogólny przykład procesu certyfikacji.

Złożenie wniosku przez administratora lub podmiot przetwarzający	Formalne sprawdzanie przez podmiot certyfikujący	Ocena Wstępna ocena	Ocena Ewaluacja przedmiotu oceny	Ocena Zatwierdzenie wyników	Informacja dla właściwego organu nadzorczego	Certyfikacja	Monitorowanie	Przedłużenie certyfikacji
Czy opis przedmiotu oceny jest jednoznaczny i kompletny, w tym w odniesieniu do interfejsów?	Czy opis przedmiotu oceny może zostać zaakceptowany?	Jakie kryteria są stosowane?	Czy przedmiot oceny spełnia kryteria?	Czy wszystkie istotne kryteria określono tak, by zdziałerciedlić przedmiot oceny?	Czy przedstawiono powody udzielenia lub cofnięcia certyfikacji?	Czy można przyznać certyfikat?	Czy przedmiot oceny w dalszym ciągu spełnia kryteria?	Czy przetwarzanie danych wciąż spełnia kryteria certyfikacji?
Czy można zapewnić dostęp do czynności przetwarzania dotyczących przedmiotu oceny?	Czy wszystkie dokumenty są kompletne i aktualne?	Jakie metody oceny są stosowane?	Czy dokumentacja dotycząca przedmiotu oceny jest prawidłowa?	Czy ocenę udokumentowano w wystarczający sposób?		Czy sprawozdania sugerowane do publikacji?	Czy certyfikat / znak jakości / znak zaufania jest poprawnie używany?	Czy podjęto zadowalające działania w odniesieniu do obszarów wymagających rozwoju?
Art. 42 ust. 6	Art. 43 ust. 4	Art. 43 ust. 4	Art. 42 ust. 5, art. 43 ust. 4	Art. 43 ust. 4	Art. 43 ust. 1, art. 43 ust. 5	Art. 43 ust. 1, art. 42 ust. 7	Art. 42 ust. 7	Art. 42 ust. 7

2 ROLA ORGANÓW NADZORCZYCH

20. Art. 42 ust. 5 stanowi, że certyfikacji dokonuje akredytowany podmiot certyfikujący lub właściwy organ nadzorczy. Zgodnie z RODO udzielanie certyfikacji nie jest obowiązkowym zadaniem organów nadzorczych. W RODO dopuszcza się natomiast wiele różnych modeli. Organ nadzorczy może na przykład wybrać co najmniej jedną z następujących możliwości:

- może sam udzielać certyfikacji na podstawie własnego systemu certyfikacji;
- może sam udzielać certyfikacji na podstawie własnego systemu certyfikacji, ale przekazać cały proces oceny lub część tego procesu osobom trzecim;

- może opracować własny system certyfikacji i powierzyć procedurę certyfikacji podmiotom certyfikującym, które będą certyfikacji udzielać; a także
- może zachęcać rynek do tworzenia mechanizmów certyfikacji.

21. Organ nadzorczy będzie również musiał rozpatrzyć swoją rolę w świetle decyzji dotyczących mechanizmów akredytacji podjętych na szczeblu krajowym – zwłaszcza jeżeli sam organ nadzorczy jest uprawniony do akredytowania podmiotów certyfikujących na podstawie art. 43 ust. 1 RODO. Tym samym każdy organ nadzorczy określi, jakie podejście przyjąć w celu realizacji szerokiego zamiaru certyfikacji na podstawie RODO. Zostanie to określone nie tylko w kontekście zadań i uprawnień wymienionych w art. 57 i 58, ale również przy uwzględnianiu certyfikacji jako czynnika, który należy brać pod uwagę przy ustalaniu administracyjnych kar pieniężnych oraz bardziej ogólnie jako sposobu wykazywania zgodności.

2.1 Organ nadzorczy jako podmiot certyfikujący

22. Jeżeli organ nadzorczy zdecyduje się na prowadzenie certyfikacji, będzie musiał starannie ocenić swoją rolę w stosunku do przypisanych mu zadań na podstawie RODO. Jego rola w wykonywaniu swoich funkcji powinna być przejrzysta. Będzie on musiał rozważyć w szczególności rozdzielenie uprawnień dotyczących postępowań i egzekwowania przepisów w celu uniknięcia wszelkich potencjalnych konfliktów interesów.

23. Działając jako podmiot certyfikujący, organ nadzorczy będzie musiał zapewnić utworzenie właściwego mechanizmu certyfikacji i opracować własne kryteria certyfikacji lub takie kryteria przyjąć. Ponadto każdy organ nadzorczy udzielający certyfikacji ma za zadanie okresowo dokonywać ich przeglądu (art. 57 ust. 1 lit. o)) oraz jest uprawniony do cofnięcia certyfikacji, jeżeli jej wymogi nie są spełnione lub przestały być spełniane (art. 58 ust. 2 lit. h)). Aby spełnić te wymogi, przydatne jest opracowanie procedury certyfikacji oraz wymogów procesu certyfikacji, a także, jeżeli nie ustalono inaczej np. w prawie krajowym, wprowadzić prawnie wiążącą umowę o świadczenie usług certyfikacyjnych z indywidualną organizacją wnioskodawcy. Należy zapewnić, by w takiej umowie dotyczącej certyfikacji wymagano od wnioskodawcy spełnienia co najmniej kryteriów certyfikacji, w tym koniecznych ustaleń dotyczących prowadzenia oceny, monitorowania spełnienia kryteriów oraz dokonywania przeglądu okresowego, w tym dostępu do informacji lub pomieszczeń, dokumentacji i publikacji sprawozdań i wyników oraz rozpatrywania skarg. Ponadto oczekuje się, że poza wymogami wymienionymi w art. 43 ust. 2 organ nadzorczy spełni wymogi określone w wytycznych w sprawie akredytacji podmiotów certyfikujących.

2.2 Dalsze zadania organu nadzorczego w odniesieniu do certyfikacji

24. W państwach członkowskich, w których podmioty certyfikujące podejmują działalność, organ nadzorczy posiada niezależnie od własnej działalności zadania i uprawnienia, takie jak:
    - ocena kryteriów systemu certyfikacji oraz przygotowanie projektu decyzji (art. 42 ust. 5);

- przekazanie EROD projektu decyzji, kiedy Rada będzie poważnie zamiar o zatwierdzeniu kryteriów certyfikacji (art. 64 ust. 1 lit. c), art. 64 ust. 7) oraz uwzględnienie opinii Rady (art. 64 ust. 1 lit. c), art. 70 ust. 1 lit. t));
- zatwierdzenie kryteriów certyfikacji (art. 58 ust. 3 lit. f)) zanim nastąpi akredytacja i certyfikacja (art. 42 ust. 5 i art. 43 ust. 2 lit. b));
- publikacja kryteriów certyfikacji (art. 43 ust. 6);
- działanie jako właściwy organ w odniesieniu do ogólnounijnych systemów certyfikacji, co może skutkować europejskim znakiem jakości ochrony danych zatwierdzonym przez EROD (art. 42 ust. 5 i art. 70 ust. 1 lit. o)); oraz a także
- nakazanie podmiotowi certyfikującemu a) nieudzielania certyfikacji lub b) cofnięcia certyfikacji, jeżeli jej wymogi (procedury dotyczące certyfikacji lub jej kryteria) nie są spełnione lub przestały być spełniane (art. 58 ust. 2 lit. h)).

25. W RODO powierza się organom nadzorczym zadanie polegające na zatwierdzaniu kryteriów certyfikacji, ale nie na opracowywaniu tych kryteriów. Aby zatwierdzić kryteria certyfikacji na podstawie art. 42 ust. 5, organ nadzorczy powinien dokładnie rozumieć, czego ma oczekiwać, zwłaszcza jeżeli chodzi o zakres oraz treść potrzebne do wykazania zgodności z RODO, oraz w odniesieniu do swojego zadania, jakim jest monitorowanie i egzekwowanie stosowania rozporządzenia. W załączniku zawarto wskazówki mające na celu zapewnienie zharmonizowanego podejścia podczas dokonywania oceny kryteriów w celu zatwierdzenia.

26. W art. 43 ust. 1 wymaga się, by podmioty certyfikujące informowały swój organ nadzorczy przed udzieleniem lub przedłużeniem certyfikacji, by umożliwić właściwemu organowi nadzorczemu wykonywanie jego uprawnień naprawczych na mocy art. 58 ust. 2 lit. h). Ponadto w art. 43 ust. 5 wymaga się również, by podmioty certyfikujące przedstawiały właściwemu organowi nadzorczemu powody udzielenia lub cofnięcia żądanej certyfikacji. Mimo że w RODO pozwala się organom nadzorczym określić, w jaki sposób będą otrzymywać informacje, uznawać je, dokonywać ich przeglądu oraz operacyjnego przetwarzania (np. może to obejmować rozwiązania technologiczne mające na celu umożliwienie realizowania sprawozdawczości przez podmioty certyfikujące), istnieje możliwość wprowadzenia procesu i kryteriów przetwarzania informacji i sprawozdań przekazanych na temat każdego udanego projektu certyfikacji przez podmiot certyfikujący zgodnie z art. 43 ust. 1. Na podstawie tych informacji organ nadzorczy może wykonać swoje uprawnienie do nakazania podmiotowi certyfikującemu cofnięcia lub nieudzielenia certyfikacji (art. 58 ust. 2 lit. h)) oraz do monitorowania i egzekwowania stosowania wymogów i kryteriów certyfikacji na podstawie RODO (art. 57 ust. 1 lit. a) i art. 58 ust. 2 lit. h)). Będzie to służyć wspieraniu zharmonizowanego podejścia oraz porównywalności w certyfikacji przez poszczególne podmioty certyfikujące oraz zapewnieniu, by informacje o statusie certyfikacji organizacji były znane organom nadzorczym.

3 ROLA PODMIOTU CERTYFIKUJĄCEGO

27. Rolą podmiotu certyfikującego jest udzielanie certyfikacji, dokonywanie ich przeglądu, przedłużanie ich i cofanie (art. 42 ust. 5 i 7) na podstawie mechanizmu certyfikacji i zatwierdzonych kryteriów (art. 43 ust. 1). Wymaga to od podmiotu certyfikującego lub właściciela systemu certyfikacji określenia i ustanowienia kryteriów i procedur certyfikacji, w tym procedur dotyczących monitorowania przestrzegania rozporządzenia, przeglądu, rozpatrywania skarg oraz cofania certyfikacji. Przeglądu kryteriów certyfikacji dokonuje się w ramach procesu akredytacji uwzględniającego zasady i procedury, na podstawie których wydaje się certyfikacje, znaki jakości i oznaczenia (art. 43 ust. 2 lit. c)).

28. Istnienie mechanizmów i kryteriów certyfikacji jest konieczne, by podmiot certyfikujący mógł otrzymać akredytację na podstawie art. 43. Istotny wpływ na to, co robi podmiot certyfikujący, wynika z zakresu i rodzaju kryteriów certyfikacji, które mają wpływ na procedury certyfikacji i vice versa. Specyficzne kryteria mogą na przykład wymagać konkretnych metod oceny, takich jak kontrole na miejscu i przegląd kodu. Procedury te są w przypadku akredytacji obowiązkowe; wyjaśniono je bardziej szczegółowo w wytycznych w sprawie akredytacji.

29. W RODO wymaga się, by podmiot certyfikujący przekazywał organom nadzorczym informacje, w szczególności na temat poszczególnych certyfikacji, które to informacje są konieczne do monitorowania stosowania mechanizmu certyfikacji (art. 42 ust. 7, art. 43 ust. 5 i art. 58 ust. 2 lit. h)).

4 ZATWIERDZENIE KRYTERIÓW CERTYFIKACJI

30. Kryteria certyfikacji stanowią integralną część każdego mechanizmu certyfikacji. W konsekwencji w RODO wymaga się zatwierdzenia kryteriów certyfikacji mechanizmu certyfikacji przez właściwy organ nadzorczy (art. 42 ust. 5 i art. 43 ust. 2 lit. b)). Natomiast w przypadku europejskiego znaku jakości ochrony danych kryteria certyfikacji zatwierdza EROD (art. 42 ust. 5 i art. 70 ust. 1 lit. o)). Obie procedury zatwierdzania kryteriów certyfikacji wyjaśniono poniżej.

31. EROD uznaje następujące cele zatwierdzania kryteriów certyfikacji:

    - odpowiednie odzwierciedlenie wymów i zasad dotyczących ochrony osób fizycznych w związku z przetwarzaniem danych osobowych, które to wymogi i zasady określono w rozporządzeniu (UE) 2016/679; a także
    - przyczynianie się do spójnego stosowania RODO.

32. Zatwierdzenia udziela się na podstawie wymogu RODO, by mechanizm certyfikacji umożliwiał administratorom i podmiotom przetwarzającym wykazanie zgodności z RODO; kryteria certyfikacji mają w pełni ten wymóg odzwierciedlać.

4.1 Zatwierdzenie kryteriów przez właściwy organ nadzorczy

33. Właściwy organ nadzorczy musi zatwierdzać kryteria certyfikacji przed rozpoczęciem procesu akredytacji podmiotu certyfikującego lub w trakcie tego procesu. Wymagane jest również zatwierdzenie zaktualizowanych lub dodatkowych systemów lub zbiorów kryteriów na

podstawie normy ISO 17065 przez ten sam podmiot certyfikujący przed zastosowaniem ich w ramach zmienionych mechanizmów certyfikacji (art. 42 ust. 5 i art. 43 ust. 2 lit. b)). Organy nadzorcze traktują wszystkie wnioski o zatwierdzenie kryteriów certyfikacji w sposób sprawiedliwy i niedyskryminujący zgodnie z publicznie dostępną procedurą określającą ogólne warunki, które należy spełnić, oraz zgodnie z opisem procesu zatwierdzania.

34. Podmiot certyfikujący może udzielać certyfikacji w danym państwie członkowskim jedynie zgodnie z kryteriami przyjętymi przez organ nadzorczy w tym państwie członkowskim. Innymi słowy, jeżeli podmiot certyfikujący zamierza oferować certyfikację i uzyska akredytację, kryteria certyfikacji musi zatwierdzać właściwy organ nadzorczy. W sekcji poniżej podano więcej informacji na temat ogólnoeuropejskich systemów certyfikacji.

4.2 Zatwierdzanie przez EROD kryteriów dotyczących europejskiego znaku jakości ochrony danych

35. Podmiot certyfikujący może również udzielać certyfikacji zgodnie z kryteriami zatwierdzonymi przez EROD w odniesieniu do europejskiego znaku jakości ochrony danych. Zatwierdzenie kryteriów certyfikacji przez EROD zgodnie z art. 63 może skutkować europejskim znakiem jakości ochrony danych (art. 42 ust. 5). W świetle istniejącej certyfikacji i konwencji w sprawie akredytacji EROD uznaje, że pożądane jest unikanie fragmentacji rynku certyfikacji ochrony danych osobowych. Rada zauważa, że art. 42 ust. 1 stanowi, iż państwa członkowskie, organy nadzorcze, Europejska Rada Ochrony Danych oraz Komisja zachęcają do ustanawiania mechanizmów certyfikacji – w szczególności na szczeblu Unii.

4.2.1 Wniosek o zatwierdzenie

36. Wniosek o zatwierdzenie przez EROD kryteriów zgodnie z art. 42 ust. 5 i art. 70 ust. 1 lit. o) musi być złożony za pośrednictwem właściwego organu nadzorczego; w takim wniosku należy określić zamiar właściciela systemu, kandydata lub akredytowanego podmiotu certyfikującego, polegający na zaoferowaniu w mechanizmie certyfikacji kryteriów, które odnosiłyby się do administratorów i podmiotów przetwarzających we wszystkich państwach członkowskich. Właściwy organ nadzorczy przekaże EROD projekt, kiedy uzna, że EROD mogłaby zatwierdzić kryteria.

37. Wybór miejsca, w którym należy złożyć wniosek o zatwierdzenie kryteriów, będzie zależał od właścicieli systemu certyfikacji lub siedziby podmiotu certyfikującego.

38. Jeżeli podmiot certyfikujący złoży wniosek, zazwyczaj będzie już trwał w odniesieniu do niego proces ubiegania się o akredytację lub podmiot ten będzie już akredytowany przez właściwy organ nadzorczy albo przez krajową jednostkę akredytującą swojego państwa członkowskiego. Jeżeli podmiot certyfikujący został już akredytowany na potrzeby mechanizmu certyfikacji RODO, może to pomóc w usprawnieniu procesu zatwierdzania.

4.2.2 Kryteria dotyczące europejskiego znaku jakości ochrony danych

39. EROD będzie koordynować proces oceny oraz zatwierdzenia europejskiego znaku jakości ochrony danych zgodnie z wymogami. Ocena będzie dotyczyła takich obszarów, jak: zakres kryteriów oraz możliwość ich wykorzystania do wspólnej certyfikacji. Oczekuje się, że jeżeli EROD zatwierdzi kryteria, organ nadzorczy właściwy dla siedziby unijnej podmiotu certyfikującego będzie rozpatrywać skargi odnoszące się do samego mechanizmu oraz poinformuje pozostałe organy nadzorcze. Ten organ nadzorczy jest również właściwy do podejmowania środków przeciwko podmiotowi certyfikującemu. W zależności od sytuacji właściwy organ nadzorczy powiadomi pozostałe organy nadzorcze oraz EROD.

40. Kryteria certyfikacji dotyczące wspólnej certyfikacji podlegają ogólnounijnym wymogom i powinny zapewniać specjalny mechanizm służący do spełnienia tych wymogów. Europejskie mechanizmy certyfikacji muszą być przeznaczone do stosowania we wszystkich państwach członkowskich. Na podstawie art. 42 ust. 5 powinno być możliwe dostosowanie mechanizmu dotyczącego europejskiego znaku jakości ochrony danych oraz jego kryteriów w taki sposób, by w stosownych przypadkach uwzględniano w nich krajowe przepisy sektorowe, np. dotyczące przetwarzania danych w szkołach; należy również brać pod uwagę zastosowanie ich w całej Europie.

41. Na przykład: międzynarodowa szkoła oferująca w Unii szkolenie osób, których dane dotyczą, znajduje się w państwie członkowskim „A". Szkoła chce poświadczyć swój proces internetowego składania wniosków za pomocą ogólnounijnego systemu certyfikacji, aby uzyskać europejski znak jakości ochrony danych. Szkoła ta ma zamiar ubiegać się o certyfikację operacji przetwarzania oferowaną przez podmiot certyfikujący ustanowiony w państwie członkowskim „B" na podstawie europejskiego znaku jakości ochrony danych. Kryteria dotyczącego tego znaku, które opracowano i udokumentowano w odpowiednim mechanizmie, muszą być w stanie uwzględnić przepisy dotyczące szkół mające zastosowanie w państwie członkowskim „A". W ramach tych kryteriów należy również wymagać stosowania przez szkołę internetowego procesu składania wniosków w celu przekazania informacji i uwzględnienia mających zastosowanie wymogów państwa członkowskiego dotyczących ochrony danych, które to wymogi mogą się różnić w zależności od państwa członkowskiego. Przykładem są zbiory danych osobowych, które mają zostać przekazane do celów wniosku, np. klasy przedszkolne lub wyniki testów, różne okresy zatrzymywania danych, gromadzenie lub przetwarzanie danych finansowych lub biometrycznych, dalsze ograniczenia w zakresie przetwarzania.

    - Ogólne kryteria dotyczące zatwierdzania mechanizmu europejskiego znaku jakości ochrony danych obejmują:
        - kryteria zatwierdzone przez Europejską Radę Ochrony Danych;
        - zastosowanie ich we wszystkich jurysdykcjach w sposób odzwierciedlający, w stosownych przypadkach, krajowe wymogi prawne i przepisy sektorowe;
        -
    - zharmonizowane kryteria, które można dostosowywać w celu odzwierciedlenia wymogów krajowych;
        - opis mechanizmu certyfikacji określający;
        - umowy w sprawie certyfikacji, w których uwzględnia się wymogi ogólnoeuropejskie;
        - procedury mające na celu zapewnienie i dostarczenie rozwiązań dla różnych krajowych uwarunkowań oraz zapewnienie, by europejski znak jakości pomagał w wykazywaniu zgodności z RODO; a także
        - język sprawozdań składanych do wszystkich odnośnych organów nadzorczych.

42. Porady dotyczące kryteriów europejskiego znaku jakości ochrony danych zawiera również załącznik.

4.2.3 Rola akredytacji

43. Jak zauważono w puncie 4.2.1, kiedy kryteria zostaną zidentyfikowane jako stosowne w odniesieniu do wspólnej certyfikacji, a Europejska Rada Ochrony Danych zatwierdzi je jako takie zgodnie z art. 42 ust. 5, podmioty certyfikujące mogą być akredytowane do prowadzenia certyfikacji na podstawie tych kryteriów na poziomie Unii.

44. Systemy, które są przeznaczone do stosowania jedynie w konkretnych państwach członkowskich, nie będą kandydatami do przyznania unijnych znaków jakości. Akredytacja w zakresie europejskiego znaku jakości ochrony danych będzie wymagała akredytacji w państwie członkowskim siedziby podmiotu certyfikującego, który ma zamiar obsługiwać system, tj. podmiotu odpowiedzialnego za udzielanie certyfikacji i zarządzanie działalnością certyfikacyjną swoich podmiotów i jednostek zależnych w innych państwach członkowskich. Jeżeli inne jednostki organizacyjne lub biura zarządzają certyfikacjami i wykonują je samodzielnie, każda z tych jednostek organizacyjnych lub biur będzie wymagać osobnej akredytacji w państwie członkowskim, w którym ma swoją siedzibę. Innymi słowy, akredytacja jest konieczna jedynie w państwie członkowskim, w którym znajduje się siedziba podmiotu certyfikującego, tylko kiedy siedziba ta wydaje certyfikaty. Natomiast, gdy inne jednostki organizacyjne podmiotu certyfikującego również wydają certyfikaty, jednostki te także muszą posiadać akredytację.

45. W związku z tym, jeżeli podmiot certyfikujący nie został akredytowany do certyfikacji w ramach europejskiego znaku jakości ochrony danych, nie mogą mieć zastosowania kryteria zatwierdzone przez EROD i nie można zaoferować znaku jakości.

5 OPRACOWYWANIE KRYTERIÓW CERTYFIKACJI

46. W RODO ustanowiono ramy opracowywania kryteriów certyfikacji. Podczas gdy do podstawowych wymogów dotyczących procedury certyfikacji odnoszą się art. 42 i 43, w których przedstawiono również kluczowe kryteria dotyczące procedur certyfikacji,

podstawa kryteriów certyfikacji musi wynikać z zasad i przepisów RODO i pomóc w zapewnieniu stosowania tych zasad i przepisów.

47. Opracowywanie kryteriów certyfikacji powinno koncentrować się na możliwości zweryfikowania, istotności i stosowności kryteriów certyfikacji do celów wykazania zgodności z rozporządzeniem. Kryteria certyfikacji powinny być sformułowane w sposób jasny i zrozumiały oraz powinny umożliwiać ich praktyczne zastosowanie.

48. Podczas opracowywania kryteriów certyfikacji należy w stosownych przypadkach brać pod uwagę następujące aspekty zgodności wspierające ocenę operacji przetwarzania danych:

    - zgodność przetwarzania z prawem, o której mowa w art. 6;
    - zasady dotyczące przetwarzania danych, o których mowa w art. 5;
    - prawa osób, których dane dotyczą, o których mowa w art. 12–23;
    - obowiązek zgłaszania naruszeń ochrony danych zgodnie z art. 33;
    - obowiązek uwzględniania ochrony danych w fazie projektowania oraz domyślną ochronę danych, zgodnie z art. 25;
    - czy w stosownych przypadkach przeprowadzono ocenę skutków dla ochrony danych zgodnie z art. 35 ust. 7 lit. d); a także
    - środki techniczne i organizacyjne wprowadzone zgodnie z art. 32.

49. Zakres, w jakim względy te odzwierciedlono w kryteriach, może być różny w zależności od zakresu certyfikacji, który może obejmować rodzaj operacji przetwarzania oraz obszar certyfikacji (np. sektor zdrowia).

5.1 Co może być przedmiotem certyfikacji na podstawie RODO?

50. EROD jest zdania, że w RODO przewidziano szeroki zakres możliwych przedmiotów certyfikacji na podstawie RODO, jeżeli nacisk kładzie się na pomoc w wykazaniu zgodności z rozporządzeniem operacji przetwarzania prowadzonych przez administratorów i podmioty przetwarzające (art. 42 ust. 1).

51. Podczas oceny operacji przetwarzania należy w stosownych przypadkach uwzględnić następujące trzy kluczowe elementy:

    1. dane osobowe (zakres przedmiotowy RODO);
    2. systemy techniczne – infrastrukturę, np. sprzęt i oprogramowanie wykorzystywane do przetwarzania danych osobowych; a także
    3. procesy i procedury związane z operacjami przetwarzania.

52. Każdy element wykorzystywany w operacjach przetwarzania musi podlegać ocenie w zestawieniu z ustalonymi kryteriami. Wpływ mogą mieć w tym przypadku co najmniej cztery różne istotne czynniki: 1) organizacja i struktura prawna administratora lub podmiotu

przetwarzającego; 2) dział, środowisko i osoby zaangażowane w operacje przetwarzania; 3) opis techniczny elementów podlegających ocenie; i wreszcie 4) infrastruktura informatyczna obsługująca operacje przetwarzania obejmująca systemy operacyjne, systemy wirtualne, bazy danych, systemy uwierzytelniania i autoryzacji, routery i zapory sieciowe, systemy magazynowania, infrastrukturę komunikacyjną lub dostęp do internetu oraz powiązane środki techniczne.

53. Wszystkie trzy podstawowe elementy są istotne przy opracowywaniu procedur i kryteriów certyfikacji. Zakres, w jakim się je uwzględnia, może różnić się w zależności od przedmiotu certyfikacji. Przykładowo w niektórych przypadkach pewne elementy można pominąć, jeżeli uzna się je za nieistotne dla przedmiotu certyfikacji.

54. W RODO zawarto dodatkowe wytyczne, na podstawie których można doprecyzować, co podlega certyfikacji na jego podstawie. Z art. 42 ust. 7 wynika, że certyfikacji na podstawie RODO udziela się wyłącznie administratorom danych i podmiotom przetwarzającym, co wyklucza między innymi możliwość udzielania certyfikacji inspektorom ochrony danych. W art. 43 ust. 1 lit. b) znajduje się odniesienie do normy ISO 17065, która przewiduję akredytację podmiotów certyfikujących dokonujących oceny wyrobów, usług i procesów. Operacja przetwarzania lub zestaw operacji mogą doprowadzić do powstania wyrobu lub usługi zgodnych z terminologią normy ISO 17065, a więc mogą być przedmiotem certyfikacji. Przykładowo przetwarzanie danych pracowników do celów wypłaty wynagrodzeń lub zarządzania urlopami w rozumieniu RODO stanowi zestaw operacji i może doprowadzić do powstania wyrobu, procesu lub usługi zgodnych z terminologią normy ISO.

55. Na podstawie powyższych ustaleń EROD uważa, że zakres certyfikacji na podstawie RODO jest ukierunkowany na operacje przetwarzania lub zestawy operacji. Powyższe może obejmować procesy zarządzania w rozumieniu środków organizacyjnych, a zatem procesy stanowiące integralne części operacji przetwarzania (np. proces zarządzania określony w odniesieniu do rozpatrywania skarg w ramach przetwarzania danych pracowników do celów wypłaty wynagrodzeń).

56. Aby ocenić zgodność operacji przetwarzania z kryteriami certyfikacji należy przedstawić przypadek użycia. Przykładowo zgodność stosowania infrastruktury technicznej wykorzystywanej w trakcie operacji przetwarzania zależy od kategorii danych, które infrastruktura ta ma przetwarzać. Stosowane środki organizacyjne zależą od kategorii i ilości danych oraz od infrastruktury technicznej wykorzystywanej do przetwarzania, z uwzględnieniem charakteru, zakresu, treści i celów przetwarzania, a także zagrożeń związanych z prawami i wolnościami osób, których dane dotyczą.

57. Ponadto należy pamiętać, że aplikacje informatyczne mogą się między sobą znacznie różnić, nawet jeśli służą tym samym celom związanym z przetwarzaniem danych. Dlatego należy to uwzględnić przy określaniu zakresu mechanizmów certyfikacji i sporządzaniu kryteriów certyfikacji, tj. zakresu certyfikacji i kryteriów nie należy zawężać tak, by spowodować wykluczenie zaprojektowanych w różny sposób aplikacji informatycznych.

5.2 Określenie przedmiotu certyfikacji

58. W przypadku poszczególnych projektów certyfikacyjnych prowadzonych w ramach mechanizmu certyfikacji należy odróżnić zakres mechanizmu certyfikacji od jej przedmiotu (zwanego również przedmiotem oceny). Mechanizm certyfikacji może określać jej zakres w sposób ogólny lub w odniesieniu do konkretnego rodzaju lub obszaru operacji przetwarzania, a zatem może już określać przedmioty certyfikacji, które mieszczą się w tym zakresie (np. bezpieczne magazynowanie i ochrona danych osobowych znajdujących się w cyfrowym sejfie). W każdym przypadku wiarygodna i sensowna ocena zgodności może mieć miejsce tylko wtedy, gdy dokładnie opisano indywidualny przedmiot projektu certyfikacyjnego. Należy jasno opisać, jakie operacje przetwarzania obejmuje przedmiot certyfikacji, po czym należy przedstawić opis podstawowych elementów, tj. które dane, procesy i infrastruktura techniczna będą poddawane ocenie, a które nie. Czyniąc to, należy zawsze również uwzględniać i opisywać powiązania z innymi procesami. Oczywiste jest, że to, czego nie wiadomo, nie może stanowić elementu oceny i w związku z tym nie może uzyskać certyfikatu. W każdym wypadku dany przedmiot certyfikacji musi być znaczący w stosunku do komunikatu lub roszczenia związanego z certyfikacją / wyrażonego za jej pośrednictwem i nie powinien wprowadzać użytkownika, klienta ani konsumenta w błąd.

59. [Przykład 1]

    Bank oferuje swoim klientom stronę internetową, dzięki której mają oni dostęp do bankowości internetowej. W ramach tej usługi istnieje możliwość wykonywania przelewów, zakupu akcji, inicjowania zleceń stałych i zarządzania rachunkiem. Bank pragnie certyfikować następujące elementy w ramach mechanizmu certyfikacji w zakresie ochrony danych osobowych, którego ogólny zakres oparto na kryteriach natury ogólnej:

    a) Bezpieczne logowanie

       Bezpieczne logowanie stanowi operację przetwarzania zrozumiałą dla użytkownika końcowego i istotną z punktu widzenia ochrony danych, ponieważ odgrywa istotną rolę w zapewnianiu bezpieczeństwa danych osobowych. W związku z tym prowadzenie tej operacji przetwarzania jest konieczne na potrzeby bezpiecznego logowania, a zatem może stanowić znaczący przedmiot oceny, jeżeli z certyfikatu jasno wynika, że certyfikuje się wyłącznie operację przetwarzania logowania.

    b) Front-end strony internetowej

       Chociaż front-end strony internetowej może być istotny z punktu widzenia ochrony danych osobowych, nie jest on zrozumiały dla użytkownika końcowego, a zatem nie może stanowić znaczącego przedmiotu oceny. Ponadto dla użytkownika nie jest jasne, jakie usługi na stronie internetowej (a zatem jakie operacje przetwarzania) obejmuje certyfikacja.

    c) Elektroniczne usługi bankowe

       Front-end i back-end strony internetowej to operacje przetwarzania wykorzystywane w ramach elektronicznych usług bankowych, które mogą mieć znaczenie dla użytkownika. W tym kontekście oba te elementy muszą być objęte przedmiotem oceny. Z przedmiotu oceny można wyłączyć operacje przetwarzania, które nie są bezpośrednio związane ze świadczeniem elektronicznych usług bankowych, takie jak operacje przetwarzania mające na celu zapobieganie praniu pieniędzy.

    Elektroniczne usługi bankowe oferowane przez bank za pośrednictwem jego strony internetowej mogą jednak również obejmować inne usługi, które z kolei wymagają prowadzenia osobnych operacji przetwarzania. W tym kontekście inne usługi mogą obejmować na przykład oferowanie produktu ubezpieczeniowego. Ponieważ ta dodatkowa usługa nie jest bezpośrednio związana z celem świadczenia elektronicznych usług bankowych, można ją wyłączyć z przedmiotu oceny. Jeżeli ta dodatkowa usługa (ubezpieczenie) jest wyłączona z przedmiotu oceny, interfejsy dla tej usługi zintegrowane ze stroną internetową są częścią przedmiotu oceny, w związku z czym należy je opisać w celu dokonania wyraźnego rozróżnienia między usługami. Sporządzenie takiego opisu jest konieczne do określenia i oceny potencjalnych przepływów danych między tymi dwoma usługami.

60. [Przykład 2]

    Bank oferuje klientom usługę umożliwiającą agregację informacji związanych z poszczególnymi rachunkami i kartami kredytowymi pochodzącymi z kilku banków (agregacja rachunków). Bank pragnie certyfikować tę usługę na podstawie RODO. Właściwy organ nadzorczy zatwierdził konkretny zestaw kryteriów certyfikacji dotyczących tego rodzaju działalności. Zakres mechanizmu certyfikacji dotyczy wyłącznie następujących aspektów zgodności:

    - uwierzytelnienie użytkownika; a także
    - akceptowalne sposoby pozyskiwania danych, które mają być agregowane, z innych banków/usług.

    Ponieważ zakres stosowania tego mechanizmu certyfikacji sam w sobie określa przedmiot oceny, nie jest możliwe znaczące zawężenie tego przedmiotu oceny w proponowanym zakresie i certyfikacja jedynie szczególnych cech lub pojedynczej czynności przetwarzania. W takim wypadku przedmiot oceny musi być równy określonemu zakresowi.

5.3 Metody ewaluacji i metodyka oceny

61. Ocena zgodności umożliwiająca wykazanie zgodności operacji przetwarzania wymaga zidentyfikowania i określenia metod ewaluacji i metodyki oceny. Istotne jest to, czy informacje wykorzystywane do oceny czerpie się wyłącznie z dokumentacji (która sama w sobie mogłaby być niewystarczająca), czy też czynnie gromadzi się je na miejscu oraz w drodze bezpośredniego lub pośredniego dostępu. Sposób gromadzenia informacji wpływa na znaczenie certyfikacji i w związku z tym należy go określić i opisać.

    Procedury udzielania i okresowego przeglądu certyfikacji powinny obejmować specyfikacje umożliwiające określenie właściwego poziomu ewaluacji (zakresu i szczegółowości) w celu spełnienia kryteriów certyfikacji. Powinny one także obejmować:

    - udzielenie informacji i przedstawienie specyfikacji zastosowanych metod oceny i ustaleń powziętych np. podczas audytów na miejscu lub pozyskanych z dokumentacji;

- przedstawienie metod ewaluacji skupiających się na operacjach przetwarzania (danych, systemów, procesów) i celu tego przetwarzania;
- określenie kategorii danych, potrzeb w zakresie ochrony oraz tego, czy zaangażowane są podmioty przetwarzające lub osoby trzecie;
- określenie ról oraz istnienia mechanizmu kontroli dostępu zdefiniowanego w odniesieniu do ról i obowiązków.

62. Zakres ewaluacji wpływa na znaczenie i wartość certyfikacji. Ograniczenie zakresu ewaluacji do celów pragmatycznych lub z myślą o obniżeniu kosztów zmniejszy znaczenie certyfikacji w zakresie ochrony danych osobowych. Z kolei decyzje dotyczące szczegółowości ewaluacji mogą przekraczać możliwości finansowe wnioskodawcy, a także często zdolność oceniających i audytorów. W celu wykazania zgodności nie zawsze kluczowe jest przeprowadzenie bardzo szczegółowej analizy wykorzystywanych systemów informatycznych, aby certyfikacja pozostała znacząca.

5.4 Dokumentacja oceny

63. Dokumentacja certyfikacyjna powinna być dokładna i wszechstronna. Brak dokumentacji oznacza, że nie można przeprowadzić właściwej oceny. Podstawową funkcją dokumentacji certyfikacyjnej jest zapewnienie przejrzystości procesu oceny w ramach mechanizmu certyfikacji. Dokumentacja dostarcza odpowiedzi na pytania dotyczące wymogów określonych w przepisach prawa. Mechanizmy certyfikacji powinny przewidywać znormalizowaną metodologię dokumentacji. W następnej kolejności ocena umożliwi porównanie dokumentacji certyfikacyjnej ze stanem faktycznym na miejscu oraz z kryteriami certyfikacji.

64. Wyczerpująca dokumentacja dotycząca tego, co już certyfikowano, oraz zastosowanej metodyki służy do zapewnienia przejrzystości. Zgodnie z art. 43 ust. 2 lit. c) mechanizmy certyfikacji powinny określać procedury umożliwiające dokonanie przeglądu certyfikacji. Aby umożliwić organowi nadzorczemu ocenę, czy i w jakim zakresie certyfikację można potwierdzić w toku formalnych postępowań wyjaśniających, szczegółowa dokumentacja może okazać się najodpowiedniejszym środkiem komunikacji. W dokumentacji przedstawionej podczas oceny należy zatem skupić się na trzech głównych aspektach:
    - zgodności i spójności stosowanych metod oceny;
    - metodach oceny mających na celu wykazanie zgodności przedmiotu certyfikacji z kryteriami certyfikacji, a zatem z rozporządzeniem; a także
    - wykazaniu, że wyniki ewaluacji zatwierdził niezależny i bezstronny podmiot certyfikujący.

5.5 Dokumentacja wyników

65. W motywie 100 przedstawiono informacje na temat celów związanych z wprowadzeniem certyfikacji.

„Aby zwiększyć przejrzystość i poprawić przestrzeganie niniejszego rozporządzenia, należy zachęcać do ustanowienia mechanizmów certyfikacji oraz do wprowadzenia znaków jakości i oznaczeń w dziedzinie ochrony danych, pozwalając w ten sposób osobom, których dane dotyczą, szybko ocenić stopień ochrony danych, której podlegają stosowne produkty i usługi."

66. W zwiększaniu przejrzystości istotną rolę odgrywa dokumentacja i informowanie o wynikach. Podmioty certyfikujące wykorzystujące mechanizmy certyfikacji, znaki jakości i oznaczenia skierowane do osób, których dane dotyczą (pełniących role konsumentów lub klientów) powinny zapewniać łatwo dostępne, zrozumiałe i stosowne informacje na temat certyfikowanych operacji przetwarzania. Te informacje publiczne powinny obejmować co najmniej:
    - opis przedmiotu oceny;
    - odniesienie do zatwierdzonych kryteriów mających zastosowanie do konkretnego przedmiotu oceny;
    - metodykę ewaluacji kryteriów (ewaluacja na miejscu, dokumentacja itd.); a także
    - okres ważności certyfikatu; a także
    - powinny zapewniać organom nadzorczym i opinii publicznej porównywalność wyników.

6 WYTYCZNE DOTYCZĄCE OKREŚLANIA KRYTERIÓW CERTYFIKACJI

67. Kryteria certyfikacji stanowią integralną część mechanizmu certyfikacji. Procedura certyfikacji obejmuje wymogi przewidujące, kto, w jaki sposób, w jakim stopniu i z jaką szczegółowością przeprowadza ocenę, która odbywa się w ramach poszczególnych projektów certyfikacyjnych dotyczących konkretnego przedmiotu oceny. Kryteria certyfikacji określają wymogi nominalne, w odniesieniu do których ocenia się rzeczywiste operacje przetwarzania zdefiniowane w ramach przedmiotu oceny. W niniejszych wytycznych dotyczących określania kryteriów certyfikacji przedstawiono ogólne wskazówki ułatwiające prowadzenie oceny kryteriów certyfikacji do celów zatwierdzenia.
    - Przy zatwierdzaniu lub określaniu kryteriów certyfikacji należy wziąć pod uwagę następujące kwestie ogólne. Kryteria certyfikacji powinny:
    - być jednorodne i możliwe do zweryfikowania;
    - być możliwe do skontrolowania w celu ułatwienia prowadzenia ewaluacji operacji przetwarzania na podstawie RODO, w szczególności poprzez określenie celów i wytycznych wykonawczych służących osiąganiu tych celów;
    - być adekwatne w odniesieniu do odbiorców docelowych (np. w relacjach B2B i między przedsiębiorstwami a konsumentami (B2C));

- uwzględniać inne normy (takie jak normy ISO, normy krajowe) i w stosownych przypadkach być z nimi interoperacyjne; a także
- być elastyczne i skalowalne w celu umożliwienia zastosowania do organizacji różnych rodzajów i rozmiarów, m.in. mikro, małych i średnich przedsiębiorstw zgodnie z art. 42 ust. 1 oraz stosowania podejścia opartego na analizie ryzyka zgodnie z motywem 77.

68. Małe przedsiębiorstwo lokalne, takie jak sprzedawca detaliczny, prowadzi zazwyczaj mniej skomplikowane operacje przetwarzania niż duży, wielonarodowy sprzedawca detaliczny. Chociaż wymogi dotyczące zgodności z prawem operacji przetwarzania są takie same, należy uwzględnić zakres przetwarzania danych i złożoność procesu przetwarzania; wynika z tego, że istnieje potrzeba, aby mechanizmy certyfikacji i ich kryteria były skalowalne w zależności od danej czynności przetwarzania.

6.1 Istniejące normy

69. Podmioty certyfikujące będą musiały rozważyć, w jaki sposób w konkretnych kryteriach uwzględnia się istniejące stosowne instrumenty, takie jak kodeksy postępowania, normy techniczne lub krajowe inicjatywy regulacyjne i prawne. Najlepiej byłoby, gdyby kryteria charakteryzowały się interoperacyjnością z istniejącymi normami mogącymi pomóc administratorowi lub podmiotowi przetwarzającemu wypełniać swoje obowiązki wynikające z RODO. Chociaż normy branżowe często skupiają się na ochronie organizacji przed zagrożeniami i ich bezpieczeństwie, RODO jest jednak ukierunkowane na ochronę praw podstawowych osób fizycznych. Przy opracowywaniu lub zatwierdzaniu kryteriów lub mechanizmów certyfikacji opartych na normach branżowych należy uwzględnić tę odmienną perspektywę.

6.2 Określenie kryteriów

70. Kryteria certyfikacji muszą odpowiadać stwierdzeniu zawartemu w certyfikacie (komunikatowi lub roszczeniu) dotyczącemu mechanizmu lub systemu certyfikacji i muszą być zgodne z oczekiwaniami, jakie ono wzbudza. Już sama nazwa mechanizmu certyfikacji może określać zakres stosowania i będzie mieć konsekwencje dla określenia kryteriów.

71. [Przykład 3]

    Mechanizm o nazwie „HealthPrivacyMark" powinien mieć zakres ograniczony do sektora zdrowia. Nazwa znaku jakości wzbudza oczekiwanie, że wymogi w zakresie ochrony danych osobowych zbadano w połączeniu z danymi dotyczącymi zdrowia. W związku z tym kryteria stosowane w ramach tego mechanizmu muszą być odpowiednie do celów oceny wymogów w zakresie ochrony danych osobowych w tym sektorze.

72. [Przykład 4]

Mechanizm, który odnosi się do certyfikacji operacji przetwarzania obejmujących systemy zarządzania przetwarzaniem danych, powinien określać kryteria pozwalające na rozpoznanie i ocenę procesów zarządzania i wspierających je środków technicznych i organizacyjnych.

73. [Przykład 5]

    Kryteria dotyczące mechanizmu, który odnosi się do przetwarzania w chmurze, muszą uwzględniać specjalne wymogi techniczne niezbędne do korzystania z usług w chmurze. Przykładowo, jeżeli wykorzystywane są serwery poza UE, kryteria muszą uwzględniać warunki określone w rozdziale V RODO w odniesieniu do przekazywania danych do państw trzecich.

74. Kryteria, które mają dotyczyć różnych przedmiotów oceny w różnych sektorach lub państwach członkowskich, powinny: umożliwiać stosowanie różnych scenariuszy; umożliwiać określanie odpowiednich środków w celu dostosowania kryteriów do małych, średnich lub dużych operacji przetwarzania i odzwierciedlać zagrożenia związane z różnym prawdopodobieństwem i wagą zagrożeń dotyczących praw i wolności osób fizycznych zgodnie z RODO. W związku z tym procedury certyfikacyjne (np. w odniesieniu do dokumentacji, badania lub zakresu i metod ewaluacji), które uzupełniają kryteria, muszą odpowiadać tym potrzebom oraz umożliwiać oraz przewidywać wprowadzenie zasad, przewidujących na przykład stosowanie odpowiednich kryteriów w poszczególnych projektach certyfikacyjnych. Kryteria muszą ułatwić przeprowadzenie oceny dotyczącej tego, czy wdrożenie odpowiednich środków technicznych i organizacyjnych zagwarantowano w wystarczającym stopniu.

6.3 Okres ważności kryteriów certyfikacji

75. Chociaż kryteria certyfikacji muszą pozostawać wiarygodne z upływem czasu, powinno się zachować w odniesieniu do nich możliwość zmiany. Podlegają one przeglądowi na przykład w sytuacji, gdy:
    - zmianie ulegną ramy prawne;
    - Trybunał Sprawiedliwości dokona w swoich orzeczeniach wykładni warunków i przepisów; lub
    - zmieni się aktualny stan wiedzy technicznej.

W imieniu Europejskiej Rady Ochrony Danych

Przewodnicząca

(Andrea Jelinek)

ZAŁĄCZNIK 1: ZADANIA I UPRAWNIENIA ORGANÓW NADZORCZYCH W ODNIESIENIU DO CERTYFIKACJI NA PODSTAWIE RODO.

	Przepisy	Wymogi
Zadania	Art. 43 ust. 6	Zobowiązuje organ nadzorczy do podania do wiadomości publicznej kryteriów, o których mowa w art. 42 ust. 5, w łatwo dostępny sposób oraz do przekazania tych kryteriów Europejskiej Radzie Ochrony Danych.
	Art. 57 ust. 1 lit. n)	Zobowiązuje organ nadzorczy do zatwierdzania kryteriów certyfikacji zgodnie z art. 42 ust. 5.
	Art. 57 ust. 1 lit. o)	Zapewnia, że gdy ma to zastosowanie (tj. gdy organ udziela certyfikacji), dokonuje on okresowego przeglądu udzielonych certyfikacji zgodnie z art. 42 ust. 7.
	Art. 64 ust. 1 lit. c)	Zobowiązuje organ nadzorczy do zgłoszenia Europejskiej Radzie Ochrony Danych projektu decyzji, w przypadku gdy zamierza zatwierdzić kryteria certyfikacji, o których mowa w art. 42 ust. 5.
Uprawnienia	Art. 58 ust. 1 lit. c)	Uprawnia organ nadzorczy do dokonywania przeglądu udzielonych certyfikacji na podstawie art. 42 ust. 7.
	Art. 58 ust. 2 lit. h)	Uprawnia organ nadzorczy do cofnięcia certyfikacji lub nakazania podmiotowi certyfikującemu cofnięcia certyfikacji, lub nakazania podmiotowi certyfikującemu nieudzielania certyfikacji.
	Art. 58 ust. 3 lit. e)	Uprawnia organ nadzorczy do akredytowania podmiotów certyfikujących.
	Art. 58 ust. 3 lit. f)	Uprawnia organ nadzorczy do udzielania certyfikacji i zatwierdzanie kryteriów certyfikacji.
	Art. 58 ust. 3 lit. e)	Uprawnia organ nadzorczy do akredytowania podmiotów certyfikujących.
	Art. 58 ust. 3 lit. f)	Uprawnia organ nadzorczy do udzielania certyfikacji i zatwierdzanie kryteriów certyfikacji.

ZAŁĄCZNIK 2

1 WPROWADZENIE

Załącznik 2 zawiera wytyczne dotyczące przeglądu i oceny kryteriów certyfikacji zgodnie z art. 42 ust. 5. W załączniku zidentyfikowano zagadnienia, które organy nadzorcze ds. ochrony danych oraz EROD wezmą pod uwagę i zastosują podczas zatwierdzania kryteriów certyfikacji dla mechanizmu certyfikacji. Pytania powinny być rozpatrywane przez podmioty certyfikujące i właścicieli systemów, którzy chcą opracować i przedstawiać kryteria zatwierdzania. Wykaz ten nie jest wyczerpujący, ale przedstawia minimum zagadnień, które należy wziąć pod uwagę. Nie wszystkie pytania będą miały zastosowanie; należy je jednak uwzględnić przy opracowywaniu kryteriów i uzasadnienia, aby wyjaśnić, dlaczego kryteria nie obejmują określonych aspektów. Niektóre pytania powtarzają się, ponieważ są zadawane w ramach różnych perspektyw. Niniejsze wytyczne należy rozpatrywać zgodnie z wymogami prawnymi przewidzianymi w RODO oraz, w stosownych przypadkach, w ustawodawstwie krajowym.

2 ZAKRES MECHANIZMU CERTYFIKACJI I PRZEDMIOT OCENY

a. Czy jasno opisano zakres mechanizmu certyfikacji (w odniesieniu do którego stosuje się kryteria ochrony danych)?

b. Czy zakres mechanizmu certyfikacji ma znaczenie dla grupy odbiorców, do której jest skierowany? Czy może wprowadzać w błąd?

- *Na przykład: Znak jakości „zaufane przedsiębiorstwo" sugeruje, że przeprowadzono kontrolę działalności w odniesieniu do całego przedsiębiorstwa, chociaż jedynie określone operacje przetwarzania danych, np. proces płatności online, faktycznie podlegają certyfikacji. W związku z tym zakres jest mylący.*

c. Czy zakres mechanizmu certyfikacji odzwierciedla wszystkie istotne aspekty operacji przetwarzania?

- *Na przykład: Znak jakości „poszanowanie życia prywatnego w dziedzinie zdrowia" musi obejmować wszystkie dane dotyczące stanu zdrowia w celu spełnienia wymogów określonych w art. 9.*

d. Czy zakres mechanizmu certyfikacji umożliwia znaczące poświadczenie ochrony danych, biorąc pod uwagę charakter, treść oraz ryzyko związane z operacjami przetwarzania?

- *Na przykład: Jeżeli zakres mechanizmu certyfikacji koncentruje się wyłącznie na określonych aspektach operacji przetwarzania danych, takich jak gromadzenie danych, ale nie na dalszych operacjach przetwarzania, takich jak przetwarzanie w celu tworzenia profili reklamowych lub zarządzanie prawami osób, których dane dotyczą, to nie jest on znaczący dla osób, których dane dotyczą.*

e. Czy zakres mechanizmu certyfikacji obejmuje przetwarzanie danych osobowych w odpowiednim kraju, w którym złożono wniosek, czy też dotyczy przetwarzania i/lub przenoszenia transgranicznego?

f. Czy kryteria certyfikacji w wystarczającym stopniu opisują sposób definiowania przedmiotu oceny?

- *Na przykład: „Marka ochrony danych osobowych" o zakresie ogólnym, która wymagałaby jedynie „specyfikacji przetwarzania będącego przedmiotem certyfikacji", nie zawierałaby wystarczająco jasnych wskazówek na temat sposobu ustalania i opisywania przedmiotu oceny.*
- *Na przykład: Szczegółowy zakres, „znaku jakości ochrony życia prywatnego dla sejfów cyfrowych" dotyczącego bezpiecznego przechowywania danych powinien szczegółowo opisywać wymogi dotyczące spełnienia tego zakresu w swoich kryteriach, np. definicję sejfu cyfrowego, wymogi dotyczące systemu oraz obowiązkowe środki techniczne i organizacyjne. W takim przypadku możliwe jest wyraźne zdefiniowanie przedmiotu oceny.*

1) Czy kryteria wymagają, aby przedmiot oceny zawierał identyfikację wszystkich istotnych operacji przetwarzania, przedstawienie przepływów danych oraz określenie obszaru zastosowania przedmiotu oceny?

   - *Na przykład: Mechanizm certyfikacji zapewnia certyfikację operacji przetwarzania danych przez administratorów danych w ramach RODO, ale nie określa obszaru zastosowania (zakres ogólny). Kryteria stosowane w ramach mechanizmu wymagają od administratora ubiegającego się o certyfikację określenia operacji przetwarzania danych (przedmiotu oceny) w odniesieniu do stosowanych rodzajów danych, systemów i procesów.*

2) Czy kryteria wymagają od wnioskodawcy wyraźnego określenia, gdzie przetwarzanie, które podlega ocenie, rozpoczyna się i kończy? Czy kryteria wymagają, aby przedmiot oceny zawierał interfejsy, w przypadku których współzależne czynności przetwarzania nie są uwzględnione jako część przedmiotu oceny? I czy jest to należycie uzasadnione?

   - *Na przykład: Przedmiot oceny opisujący w sposób wystarczająco szczegółowy proces przetwarzania usługi sieciowej, takiej jak rejestracja użytkowników, świadczenie usług, fakturowanie, rejestrowanie adresów IP, interfejsy z użytkownikami oraz stronami trzecimi, z wyłączeniem hostingu serwerów (ale włączając umowy w sprawie przetwarzania oraz środków technicznych i organizacyjnych).*

g. Czy kryteria gwarantują, że poszczególne przedmioty oceny są zrozumiałe dla odbiorców, w tym w stosownych przypadkach osób, których dane dotyczą?

3 WYMOGI OGÓLNE

a. Czy wszystkie terminy stosowane w katalogu kryteriów (tj. pełny zestaw kryteriów certyfikacji) zostały określone, wyjaśnione i opisane?

b. Czy zidentyfikowano wszystkie odniesienia normatywne?

c. Czy kryteria obejmują definicję obowiązków, procedur i operacji przetwarzania w zakresie ochrony danych objętych zakresem stosowania mechanizmu certyfikacji?

4 OPERACJA PRZETWARZANIA, ART. 42 UST. 1

W odniesieniu do zakresu mechanizmu certyfikacji (ogólnego lub szczególnego), czy wszystkie istotne elementy operacji przetwarzania danych (dane, systemy i procesy) zostały uwzględnione w kryteriach?

a. Czy kryteria wymagają zidentyfikowania ważnych podstaw prawnych przetwarzania danych w odniesieniu do przedmiotu oceny?

b. Czy, w odniesieniu do przedmiotu oceny, kryteria uwzględniają odpowiednie fazy przetwarzania danych i cały cykl życia danych, w tym ich usunięcie i anonimizację?

c. Czy, w odniesieniu do przedmiotu oceny, kryteria wymagają możliwości przenoszenia danych?

d. Czy, w odniesieniu do przedmiotu oceny, kryteria pozwalają na zidentyfikowanie i odzwierciedlenie szczególnych rodzajów operacji przetwarzania danych, np. automatycznego podejmowania decyzji, profilowania?

e. Czy, w odniesieniu do przedmiotu oceny, kryteria pozwalają na określenie szczególnych kategorii danych?

f. Czy kryteria przewidują (wymagają) oceny ryzyka poszczególnych operacji przetwarzania oraz potrzeb w zakresie ochrony praw i wolności osób, których dane dotyczą?

g. Czy kryteria przewidują (wymagają) odpowiednie uwzględnienie zagrożeń dla praw i wolności osób fizycznych?

...

5 ZGODNOŚĆ PRZETWARZANIA Z PRAWEM

a. Czy kryteria wymagają sprawdzenia zgodności z prawem przetwarzania danych dla poszczególnych operacji przetwarzania w odniesieniu do celu i konieczności przetwarzania?

b. Czy kryteria wymagają sprawdzenia wszystkich wymogów podstawy prawnej dla poszczególnych operacji przetwarzania?

6 ZASADY, ART. 5

a. Czy kryteria uwzględniają w odpowiedni sposób wszystkie zasady ochrony danych zgodnie z art. 5?

b. Czy kryteria wymagają wykazania poszanowania zasady minimalizacji danych dla poszczególnych przedmiotów oceny?

...

7 OGÓLNE OBOWIĄZKI ADMINISTRATORÓW I PODMIOTÓW PRZETWARZAJĄCYCH

a. Czy kryteria wymagają potwierdzenia porozumień umownych między podmiotami przetwarzającymi a administratorami danych?

b. Czy umowy między podmiotami przetwarzającymi a administratorami danych są przedmiotem oceny?

c. Czy kryteria odzwierciedlają obowiązki administratora wynikające z rozdziału IV?

d. Czy kryteria wymagają dowodu dokonania przeglądu i aktualizacji środków technicznych i organizacyjnych wprowadzonych przez administratora zgodnie z art. 24 ust. 1?

e. Czy kryteria obejmują sprawdzenie, czy organizacja dokonała oceny stosowności wyznaczenia inspektora ochrony danych zgodnie z wymogami art. 37? W stosownych przypadkach czy inspektor ochrony danych spełnia wymogi określone w art. 37 – 39?

f. Czy kryteria obejmują sprawdzenie, czy rejestry czynności przetwarzania danych są wymagane zgodnie z art. 30 ust. 5 i w odpowiedni sposób uwzględniają wymogi określone w art. 30?

8 PRAWA OSÓB, KTÓRYCH DANE DOTYCZĄ

a. Czy kryteria w odpowiedni sposób odnoszą się do prawa osób, których dane dotyczą, do informacji oraz wymagają wprowadzenia odpowiednich środków?

b. Czy kryteria wymagają, aby osobom, których dane dotyczą, przyznano odpowiedni, a nawet wyższy poziom dostępu i kontroli do ich danych, w tym możliwość przenoszenia danych?

c. Czy kryteria wymagają wprowadzenia środków przewidujących możliwość interwencji w ramach operacji przetwarzania w celu zagwarantowania praw osób, których dane dotyczą, oraz umożliwienia wprowadzania korekt, ograniczeń lub usuwania danych?

...

9 RYZYKO NARUSZENIA PRAW LUB WOLNOŚCI OSÓB FIZYCZNYCH

a. Czy kryteria przewidują (wymagają) dokonanie oceny zagrożeń dla praw i wolności osób fizycznych?

b. Czy kryteria przewidują lub wymagają zastosowania uznanej metodyki oceny ryzyka? W stosownych przypadkach, czy jest to współmierne?

c. Czy kryteria przewidują (wymagają) dokonanie oceny wpływu przewidywanych operacji przetwarzania na prawa i wolności osób fizycznych?

d. Czy kryteria wymagają uprzedniej konsultacji w sprawie pozostałych czynników ryzyka, które nie mogłyby zostać ograniczone na podstawie wyników oceny skutków dla ochrony danych?

10 ŚRODKI TECHNICZNE I ORGANIZACYJNE GWARANTUJĄCE OCHRONĘ

a. Czy kryteria wymagają zastosowania środków technicznych i organizacyjnych zapewniających poufność operacji przetwarzania?

b. Czy kryteria wymagają zastosowania środków technicznych i organizacyjnych zapewniających integralność operacji przetwarzania?

c. Czy kryteria wymagają zastosowania środków technicznych i organizacyjnych zapewniających dostępność operacji przetwarzania?

d. Czy kryteria wymagają zastosowania środków zapewniających przejrzystość operacji przetwarzania w odniesieniu do:

e. rozliczalności?

f. praw osób, których dane dotyczą?

g. oceny poszczególnych operacji przetwarzania, np. w odniesieniu do przejrzystości algorytmów?

h. Czy kryteria wymagają zastosowania środków technicznych i organizacyjnych gwarantujących prawa osób, których dane dotyczą, np. możliwości dostarczania informacji lub przenoszenia danych?

i. Czy kryteria wymagają zastosowania środków technicznych i organizacyjnych zapewniających możliwość interwencji w ramach operacji przetwarzania w celu zagwarantowania praw osób, których dane dotyczą, oraz umożliwienia wprowadzania korekt, ograniczeń lub usuwania danych?

j. Czy kryteria wymagają zastosowania środków zapewniających możliwość interwencji w ramach operacji przetwarzania w celu w celu naprawienia lub sprawdzenia systemu lub procesu?

k. Czy kryteria wymagają zastosowania środków technicznych i organizacyjnych w celu zapewnienia minimalizacji danych, na przykład niełączenia lub oddzielenia danych od podmiotu danych, anonimizacji lub pseudonimizacji lub izolacji systemów danych?

l. Czy kryteria wymagają zastosowania środków technicznych w celu wdrożenia domyślnej ochrony danych?

m. Czy kryteria wymagają środków technicznych i organizacyjnych wdrażających ochronę danych już w fazie projektowania, np. system zarządzania ochroną danych w celu wykazania, kontroli i egzekwowania wymogów ochrony danych oraz informowania o nich?

n. Czy kryteria wymagają środków technicznych i organizacyjnych wdrażających odpowiednie okresowe szkolenia dla personelu mającego stały lub regularny dostęp do danych osobowych?

o. Czy kryteria wymagają przeglądu środków?

p. Czy kryteria wymagają samooceny/audytu wewnętrznego?

q. Czy kryteria wymagają zastosowania środków w celu zapewnienia, by obowiązki w zakresie powiadamiania o naruszeniu ochrony danych osobowych były wykonywane w odpowiednim czasie i zakresie?

r. Czy kryteria wymagają wprowadzenia i weryfikacji procedur zarządzania incydentami?

s. Czy kryteria wymagają monitorowania zmian związanych z prywatnością i technologią oraz aktualizacji programu w razie potrzeby?

...

11 INNE CECHY SZCZEGÓLNE SPRZYJAJĄCE OCHRONIE DANYCH

a. Czy kryteria wymagają wdrożenia technik służących poprawie ochrony danych? Może to obejmować kryteria, które wymagają zwiększonej ochrony danych poprzez wyeliminowanie lub ograniczenie danych osobowych, lub czynniki ryzyka dla ochrony danych.

- *Na przykład: Kryteria wymagające większego stopnia niepołączalności danych poprzez wykorzystanie rozwiązań zarządzania tożsamością zorientowanych na użytkownika, takich jak dane uwierzytelniające oparte na atrybutach (ABC), zamiast rozwiązań*

zarządzania tożsamością zorientowanych na organizację, odzwierciedlałyby technikę wzmacniającą ochronę danych.

b. Czy kryteria wymagają wdrożenia wzmocnionych kontroli ze strony osób, których dane dotyczą w celu ułatwienia samostanowienia i wyboru?

...

12 KRYTERIA SŁUŻĄCE WYKAZANIU ISTNIENIA ODPOWIEDNICH ZABEZPIECZEŃ W ODNIESIENIU DO PRZEKAZYWANIA DANYCH OSOBOWYCH

Kryteria zostaną uwzględnione w przyszłych wytycznych w sprawie art. 42 ust. 2.

13 DODATKOWE KRYTERIA DOTYCZĄCE EUROPEJSKIEGO ZNAKU JAKOŚCI OCHRONY DANYCH

a. Czy kryteria obejmują wszystkie państwa członkowskie?

b. Czy kryteria umożliwiają uwzględnienie przepisów lub scenariuszy danego państw członkowskich dotyczących ochrony danych?

c. Czy kryteria wymagają dokonania oceny poszczególnych przedmiotów oceny w odniesieniu do przepisów dotyczących ochrony danych obowiązujących w danym sektorze w danym państwie członkowskim?

d. Czy kryteria wymagają od administratora lub podmiotu przetwarzającego dostarczania informacji osobom, których dane dotyczą, oraz zainteresowanym stronom, w językach państw członkowskich:

e. informacje w sprawie przetwarzania/przedmiotu oceny?

f. dokumentacja dotycząca przetwarzania/przedmiotu oceny?

g. wyniki oceny?

...

14 OGÓLNA OCENA KRYTERIÓW

a. Czy kryteria w pełni obejmują zakres mechanizmu certyfikacji (tj. kryteria kompleksowe), zapewniając tym samym wystarczające gwarancje, aby można było zaufać certyfikacji?

- *Na przykład: Jeżeli zakres mechanizmu certyfikacji koncentruje się na operacjach przetwarzania danych dotyczących zdrowia, należy zagwarantować wysoki poziom ochrony danych, określając kryteria zapewniające np. pogłębioną ocenę i stosowanie zasad ochrony prywatności już w fazie projektowania oraz domyślnej prywatności.*

b. Czy kryteria są proporcjonalne do rozmiaru czynności przetwarzania objętych zakresem mechanizmu certyfikacji, do wrażliwość informacji i do ryzyka związanego z przetwarzaniem?

c. Czy kryteria mogą poprawić przestrzeganie przepisów dotyczących ochrony danych przez administratorów i podmioty przetwarzające?

d. Czy osoby, których dane dotyczą, będą mogły korzystać z przysługujących im praw do informacji, w tym z objaśnienia im pożądanych wyników?



Recommendations 02/2021 on the legal basis for the storage of credit card data for the sole purpose of facilitating further online transactions

Adopted on 19 May 2021

The European Data Protection Board

Having regard to Article 70(1)(e) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,

Having regard to Article 12 and Article 22 of its Rules of Procedure,

HAS ADOPTED THE FOLLOWING RECOMMENDATIONS:

1. In the context of the COVID-19 pandemic the digital economy and e-commerce continuously developed. Analogously the risks of using credit card data online has increased. As stated by the Article 29 Working Party in its guidelines on Data Protection Impact Assessments, credit card data violations "*clearly involves serious impacts in the data subject's daily life*", as financial data can be used for "*payment fraud*"[1].

2. Therefore, it is very important that controllers put in place the appropriate safeguards for the data subjects, and to ensure them the control over their personal data, in order to decrease the risk of unlawful processing and foster trust in the digital environment. The EDPB deems this trust vital for sustainable growth of the digital economy.

3. For this purpose, these recommendations aim to encourage a harmonised application of data protection rules regarding the processing of credit card data within the European Economic Area (EEA), and to guarantee a homogeneous protection of data subject's rights, in full respect of the fundamental data protection principles as required by the GDPR.

4. More specifically, these recommendations deal with the storing of credit card data by online providers of goods and services, for the sole and specific purpose of facilitating further purchases by data subjects[2]. They cover the situation where a data subject buys product or pays for a service via a website or an application, and provides his/her credit card data, generally on a dedicated form, in order to conclude this unique transaction.

5. As with any processing, the controller must have a valid legal basis under Art 6 GDPR to store those data. In this regard, it should be noted that a number of the legal bases mentioned in Article 6 GDPR would not be applicable to this situation and have to be excluded. The storage of credit card data following a transaction, in order to facilitate further purchases, cannot be considered necessary for compliance with a legal obligation (Art. 6(1)(c) GDPR) nor to protect the vital interest

[1] ARTICLE 29 DATA PROTECTION WORKING PARTY - Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679.
[2] It should be noted that they do not cover payment institutions operating in online stores, nor public authorities. Neither the storage of credit card data for any other purpose, for instance for compliance with a legal obligation, or to establish a recurring payment in cases of contract of continuing performance or subscription for a long-term service (e.g. a contract which stipulates the supply of a certain good every month, or the subscription for a music or movie streaming service).

of a natural person (Art. 6(1)(d) GDPR). The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (Art. 6(1)(e) GDPR) cannot be considered as an adequate legal basis either.

6. In addition, the storage of the credit card data after the payment for goods or services is not, as such, necessary for the performance of a contract (Art. 6(1)(b) GDPR). Whereas, in the first place, the processing of the data related to the credit card used by the client to pay is necessary to fulfil the contract, thereby triggering Article 6 (1)(b) GDPR, the storage of these data is only useful in order to facilitate the potential next transaction and facilitate the sales. Such purpose cannot be considered as strictly necessary for the performance of the contract for the provision of the good or service that the data subject has already paid[3].

7. When it comes to a processing necessary for the purposes of the legitimate interest of the controller or a third party[4], the EDPB notes that for the controller to be able to rely on Article 6(1)(f) GDPR, the three conditions laid down by this article must be satisfied[5]. This legal basis requires, first, the identification and qualification of a legitimate interest pursued by the controller or by a third party. The interest of the controller or third party may be broader than the purpose of the processing and must be present and effective at the date of the data processing[6].

8. The legitimate interest legal basis requires, second, the need to process personal data for the purposes of the legitimate interest pursued. For what regards this last condition, provided that the controller has a legitimate interest as outlined above, it is not evident that the storage of the credit card data to facilitate future purchases is necessary to pursue that legitimate interest. Indeed, the actual conclusion of another purchase depends on the consumer choice and is not determined by the possibility to realize it "in one click".

9. Finally, the third condition requires the performance of a balancing test: the legitimate interest of the controller or third party must be balanced against the interests or fundamental rights and freedoms of the data subject, including data subject rights to data protection and privacy. The balancing test requires taking into consideration the particular circumstances of the processing[7]. An essential component of the balancing exercise is the potential impact on the data subject's rights and freedoms resulting from the processing[8]. Such impact can depend on the nature of data, specific method of processing and access to such data by third parties. Regarding the nature of

[3] See as well EDPB Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subject, in particular on page 10.
[4] See Article 29 Working Party Opinion on the notion of legitimate interest of the data controller under Article 7 of Directive 95/46/EC, currently under revision by the EDPB (see the EDPB Work program 2021/2022 adopted on the 16 March 2021).
[5] See CJEU judgement of 4 May 2017, Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA 'Rīgas satiksme', Case C-13/16, ECLI:EU:C:2017:336, point 28.
[6] See CJEU judgement of 11 December 2019, TK v Asociația de Proprietari bloc M5A-ScaraA, Case C-708/18, ECLI:EU:C:2019:1064, point 44.
[7] See CJEU judgement of 24 November 2011, Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v Administración del Estado, Cases C-468/10 and C-469/10, ECLI:EU:C:2011:777, points 47 and 48; CJEU judgement of 19 October 2016, Patrick Breyer v Bundesrepublik Deutschland, Case C-582/14, ECLI:EU:C:2016:779, point 62.
[8] See CJEU judgement of 24 November 2011 abovementioned, point 44; CJEU judgement of 11 December 2019 abovementioned, point 56.

data criterion, it should be noted that financial data have been qualified by the Article 29 Working Party as data of a highly personal nature because their violation clearly involves serious impacts in on the data subject's daily life[9]. Hence, notwithstanding the controller's obligation to implement technical and organisational measures to ensure appropriate security of the credit card data pursuant to Article 5(1)(f) GDPR and the fact that those data may be stored for other purposes, their processing to facilitate further purchases may involve an increasing risk of credit card data security breaches as it implies processing in other systems. Another important element of the balancing test that could be taken into consideration to assess the impact of the processing on data subjects' is the reasonable expectations of data subjects based on their relationship with the data controller, the context and the purpose of personal data collection[10]. Yet, it appears that at the time of purchase, while providing credit card data for the payment, the data subject does not reasonably expect his or her credit card data to be stored for longer than what is necessary to pay the goods or services he/she is buying. Consequently, the fundamental rights and freedoms of the person concerned by the data protection would likely take precedence over the controller's interest in this specific context.

10. Those aspects lead to conclude that consent (Art. 6(1)(a) GPDR) appears to be the sole appropriate legal basis for the above-described processing to be lawful. Indeed, to address the security risks, to allow the data subject to keep control over his/her data, and to decide actively of the use of his/her credit data, the specific consent of the data subject should be obtained before storing his or her credit card data after a purchase. This consent will enable the controller to demonstrate the individual's willingness to facilitate his/her further purchases through the specific website or application, which cannot be presumed by the simple fact he/she concluded one, or several, isolated transactions.

11. This consent cannot be presumed, it must be free, specific, informed and unambiguous[11]. It must be delivered by a clear affirmative action, and should be requested in a user-friendly way, such as through a checkbox, which should not be pre-ticked[12], directly on the form used for the data collection. This specific consent must be distinguished from the consent given for terms of service or of sales and not be a condition to the completion of the transaction.

12. According to the Article 7(3) GDPR, the data subject shall have the right to withdraw his or her consent for the storing of credit card data for the purposes of facilitating further purchases at any time. The withdrawal must be free, simple and as easy for the data subject, as it was to give consent. It must lead to the effective deletion by the controller of credit card data stored for the sole purpose of facilitating further transactions.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

[9] ARTICLE 29 DATA PROTECTION WORKING PARTY - Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679.
[10] See recital 47 GDPR.
[11] See EDPB Guidelines 05/2020 on consent under Regulation 2016/679.
[12] *ibid*.



Zalecenia 01/2021 w sprawie odpowiedniego stopnia ochrony przekazywanych danych osobowych na mocy dyrektywy (UE) 2016/680

przyjęte 2 lutego 2021 r.

Historia wersji

Wersja 1.1	6 lipca 2021 r.	Zmiana formatowania
Wersja 1.0	2 lutego 2021 r.	Przyjęcie zaleceń

Spis treści

1. WPROWADZENIE 4
2. POJĘCIE ODPOWIEDNIEGO STOPNIA OCHRONY 5
3. ASPEKTY PROCEDURALNE ZWIĄZANE Z USTALENIAMI DOTYCZĄCYMI ZAPEWNIENIA ODPOWIEDNIEGO STOPNIA OCHRONY NA PODSTAWIE DYREKTYWY 2016/680 7
4. UNIJNE NORMY DOTYCZĄCE ODPOWIEDNIEGO STOPNIA OCHRONY W ZAKRESIE WSPÓŁPRACY POLICYJNEJ I WSPÓŁPRACY WYMIARÓW SPRAWIEDLIWOŚCI W SPRAWACH KARNYCH 8
A. Zasady ogólne i zabezpieczenia 11
a) Pojęcia 11
b) Zgodność z prawem i rzetelność przetwarzania danych osobowych 11
c) Zasada ograniczenia celu 12
d) Szczególne warunki dalszego przetwarzania do innych celów 13
e) Zasada minimalizacji danych 13
f) Zasada prawidłowości danych 13
g) Zasada zatrzymywania danych 13
h) Zasada bezpieczeństwa i poufności 14
i) Zasada przejrzystości (art. 13, motywy 26, 39, 42, 43, 44, 46) 14
j) Prawo dostępu, prawo do sprostowania i usunięcia danych (art. 14 i 16) 14
k) Ograniczenia praw osoby, której dane dotyczą 15
l) Ograniczenie dalszego przekazywania danych (art. 35, motywy 64–65) 15
m) Zasada rozliczalności 16
B. Przykłady dodatkowych zasad, które mają być stosowane do konkretnych rodzajów przetwarzania 17
a) Szczególne kategorie danych 17
b) Zautomatyzowane podejmowanie decyzji i profilowanie 17
c) Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych 17
C. Mechanizmy proceduralne i mechanizmy egzekwowania prawa 18
a) Właściwy niezależny organ nadzorczy 18
b) Skuteczne wdrażanie przepisów dotyczących ochrony danych 18
c) System ochrony danych ułatwia wykonywanie praw osobie, której dane dotyczą 18
d) System ochrony danych zapewnia odpowiednie mechanizmy dochodzenia roszczeń 19

Europejska Rada Ochrony Danych,

uwzględniając art. 51 ust. 1 lit. b) dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylającej decyzję ramową Rady 2008/977/WSiSW[1],

uwzględniając art. 12 i 22 swojego regulaminu wewnętrznego,

PRZYJMUJE NINIEJSZE ZALECENIA:

1. WPROWADZENIE

1. Grupa Robocza Art. 29 opublikowała dokument roboczy[2] w sprawie odpowiedniego stopnia ochrony przekazywanych danych osobowych na mocy ogólnego rozporządzenia o ochronie danych (RODO)[3]. Dokument ten został zatwierdzony przez Europejską Radę Ochrony Danych (EROD) na pierwszej sesji plenarnej.

2. Zgodnie z deklaracją nr 21 dołączoną do Traktatu z Lizbony konieczne może okazać się wprowadzenie zasad szczególnych dotyczących ochrony danych osobowych i swobodnego przepływu tych danych w dziedzinach współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej, zapewnianej na podstawie art. 16 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE), ze względu na szczególny charakter tych dziedzin.

3. Na tej podstawie prawodawca UE przyjął dyrektywę (UE) 2016/680 ustanawiającą przepisy szczególne dotyczące przetwarzania danych osobowych przez właściwe organy do celów **zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom**.

4. W tym kontekście dyrektywa 2016/680 określa podstawy umożliwiające przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych. Jedną z podstaw tego rodzaju przekazywania danych jest decyzja Komisji Europejskiej stwierdzająca, że dane państwo trzecie lub organizacja międzynarodowa zapewniają odpowiedni stopień ochrony.

[1] Dz.U. L 119 z 4.5.2016, s. 89.
[2] Dokument WP254.rev01 przyjęty przez Grupę Roboczą Art. 29 w dniu 28 listopada 2017 r., ostatnio zmieniony i przyjęty w dniu 6 lutego 2018 r. Stanowi on aktualizację rozdziału I dokumentu roboczego WP12 „Przekazywanie danych osobowych do państw trzecich: stosowanie art. 25 i 26 unijnej dyrektywy o ochronie danych" (ang. Transfer of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive) przyjętego przez Grupę Roboczą Art. 29 w dniu 24 lipca 1998 r.
[3] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), Dz.U. L 119 z 4.5.2016, s. 1.

5. Dokument roboczy WP254.rev01 w sprawie odpowiedniego stopnia ochrony przekazywanych danych osobowych ma na celu przekazanie Komisji Europejskiej wytycznych dotyczących stopnia ochrony danych osobowych w państwach trzecich i organizacjach międzynarodowych na podstawie RODO, natomiast niniejszy dokument ma na celu zapewnienie podobnych wytycznych na podstawie dyrektywy 2016/680. W tym kontekście określa się w nim podstawowe zasady ochrony danych, które muszą być zawarte w ramach prawnych państwa trzeciego lub organizacji międzynarodowej w celu zapewnienia merytorycznej równoważności z ramami UE w zakresie dyrektywy 2016/680 (tj. w odniesieniu do przetwarzania danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar). Ponadto niniejszy dokument może zapewnić wskazówki państwom trzecim i organizacjom międzynarodowym zainteresowanym uzyskaniem odpowiedniego stopnia ochrony.

6. Niniejszy dokument dotyczy wyłącznie decyzji stwierdzających odpowiedni stopień ochrony. Są to akty wykonawcze Komisji Europejskiej przyjmowane zgodnie z art. 36 ust. 3 dyrektywy 2016/680.

2. POJĘCIE ODPOWIEDNIEGO STOPNIA OCHRONY

7. Dyrektywa 2016/680 określa zasady przekazywania danych osobowych do państw trzecich i organizacji międzynarodowych w zakresie, w jakim takie przekazywanie danych wchodzi w zakres jej stosowania. Przepisy dotyczące międzynarodowego przekazywania danych osobowych określono w rozdziale V dyrektywy 2016/680, w szczególności w jej art. 35–39.

8. Na podstawie art. 36 dyrektywy 2016/680 przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej może nastąpić, jeżeli państwo trzecie, terytorium lub przynajmniej jeden sektor w tym państwie trzecim, lub organizacja międzynarodowa zapewniają odpowiedni stopień ochrony. Z orzecznictwa Trybunału Sprawiedliwości Unii Europejskiej (TSUE)[4] wynika, że przepis ten należy interpretować w świetle art. 35 dyrektywy 2016/680, zatytułowanego „Ogólne zasady przekazywania danych osobowych", który stanowi, że „wszystkie przepisy [rozdziału V tej dyrektywy] stosuje się w celu zapewnienia, by stopień ochrony osób fizycznych zapewniony niniejszą dyrektywą nie został obniżony".

9. W przypadku gdy Komisja Europejska zdecydowała, że taki odpowiedni stopień ochrony jest zapewniony, przekazywanie danych osobowych do tego państwa trzeciego, terytorium, sektora lub organizacji międzynarodowej może nastąpić bez konieczności uzyskania specjalnego zezwolenia, z wyjątkiem sytuacji, w której inne państwo członkowskie, od którego uzyskano dane, musi udzielić zezwolenia na przekazanie, jak przewidziano w art. 35 i 36 oraz w motywie 66 dyrektywy 2016/680. Nie wpływa to na konieczność zapewnienia, by przetwarzanie danych przez organy zainteresowanych państw członkowskich było zgodne z przepisami krajowymi przyjętymi na podstawie dyrektywy (UE) 2016/680.

[4] Sprawa C-311/18, Data Protection Commissioner przeciwko Facebook Ireland Ltd i Maximillian Schrems, wyrok z dnia 16 lipca 2020 r., ECLI:EU:C:2020:559, pkt 92 (Schrems II).

10. Pojęcie „odpowiedniego stopnia ochrony", które istniało już na mocy dyrektywy 95/46/WE[5] i decyzji ramowej Rady 2008/977/WSiSW[6], zostało doprecyzowane w tym kontekście przez TSUE, a ostatnio w ramach RODO.

11. Jak wyjaśnił TSUE, o ile stopień ochrony w państwie trzecim musi być merytorycznie równoważny temu gwarantowanemu w UE, „środki, z jakich to państwo trzecie korzysta w tym względzie dla zapewnienia takiego stopnia ochrony, mogą różnić się od środków wprowadzonych w Unii", ale „środki te powinny w praktyce skutecznie zapewniać ochronę"[7]. W związku z powyższym norma dotycząca odpowiedniego stopnia ochrony danych nie wymaga dokładnego powielania przepisów unijnych, ale ustanowienia zasadniczych, tj. podstawowych, wymogów określonych w tych przepisach.

12. W tym kontekście Trybunał wyjaśnił również, że decyzja Komisji stwierdzająca odpowiedni stopień ochrony powinna zawierać wszelkie stwierdzenia dotyczące istnienia w państwie trzecim przepisów służących ograniczeniu ewentualnych ingerencji w prawa podstawowe osób, których dane zostały przekazane z Unii do tego państwa trzeciego, ingerencji, których organy państwowe tego kraju *mogłyby* dokonywać przy okazji dążenia do realizacji uzasadnionego prawem celu, takiego jak bezpieczeństwo narodowe[8].

13. Celem decyzji Komisji Europejskiej stwierdzających odpowiedni stopień ochrony jest formalne potwierdzenie ze skutkiem wiążącym dla państw członkowskich[9], w tym dla ich właściwych organów ochrony danych[10], że stopień ochrony danych osobowych w państwie trzecim lub organizacji międzynarodowej jest merytorycznie równoważny stopniowi ochrony danych osobowych w Unii Europejskiej. Państwo trzecie powinno dawać gwarancje zapewniające odpowiedni stopień ochrony, zasadniczo odpowiadający stopniowi przewidzianemu w Unii, w szczególności gdy dane są przetwarzane w jednym konkretnym sektorze lub większej ich liczbie[11].

14. Odpowiedni stopień ochrony można osiągnąć przez połączenie praw osób, których dane dotyczą, i obowiązków podmiotów, które przetwarzają dane lub sprawują kontrolę nad takim przetwarzaniem i nadzorem ze strony niezależnych organów. Przepisy o ochronie danych są jednak skuteczne tylko wtedy, gdy są możliwe do wyegzekwowania na drodze prawnej i przestrzegane w praktyce. Konieczne jest zatem rozważenie nie tylko treści przepisów mających zastosowanie do danych osobowych przekazywanych do państwa trzeciego lub organizacji międzynarodowej, ale także systemu stworzonego w celu zapewnienia skuteczności tych przepisów. Skuteczne mechanizmy egzekwowania prawa mają nadrzędne znaczenie dla skuteczności przepisów o ochronie danych[12].

[5] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, Dz.U. L 281 z 23.11.1995, s. 31.

[6] Decyzja ramowa Rady 2008/977/WSiSW z dnia 27 listopada 2008 r. w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych, Dz.U. L 350 z 30.12.2008, s. 60.

[7] Sprawa C-362/14, Maximillian Schrems przeciwko Data Protection Commissioner, wyrok z dnia 6 października 2015 r., ECLI:EU:C:2015:650, pkt 73 i 74 (Schrems I).

[8] Schrems I, pkt 88.

[9] Art. 288 TFUE.

[10] Schrems I, pkt 52.

[11] Motyw 67 dyrektywy 2016/680.

[12] Schrems I, pkt 72–74 oraz opinia TSUE 1/15 w sprawie projektu umowy między Kanadą a Unią Europejską, z dnia 26 lipca 2017 r., ECLI:EU:C:2017:592 (opinia 1/15), pkt 134: „Rzeczone prawo do ochrony danych osobowych wymaga w szczególności, by ciągłość wysokiego poziomu ochrony praw i wolności przyznanego

3. ASPEKTY PROCEDURALNE ZWIĄZANE Z USTALENIAMI DOTYCZĄCYMI ZAPEWNIENIA ODPOWIEDNIEGO STOPNIA OCHRONY NA PODSTAWIE DYREKTYWY 2016/680

15. Aby EROD mogła wypełnić swoje zadanie polegające na doradzaniu Komisji Europejskiej zgodnie z art. 51 ust. 1 lit. g) dyrektywy 2016/680, powinna otrzymać odpowiednią dokumentację, w tym odpowiednią korespondencję i ustalenia dokonane przez Komisję Europejską. Bezwzględnie konieczne jest, aby wszelkie istotne dokumenty były przekazywane EROD z odpowiednim wyprzedzeniem, w tłumaczeniu na język angielski, aby przed ostatecznym przyjęciem decyzji stwierdzającej odpowiedni stopień ochrony możliwe było przeprowadzenie merytorycznych i owocnych dyskusji. W przypadku gdy ramy prawne są złożone, dokumentacja taka powinna obejmować wszelkie przygotowane sprawozdania na temat stopnia ochrony danych osobowych w państwie trzecim lub organizacji międzynarodowej. W każdym razie informacje dostarczone przez Komisję Europejską powinny być wyczerpujące i powinny umożliwić EROD dokonanie oceny analizy przeprowadzonej przez Komisję w zakresie stopnia ochrony danych osobowych w państwie trzecim lub organizacji międzynarodowej.

16. EROD przedstawi w odpowiednim czasie opinię na temat ustaleń Komisji Europejskiej, wskazując możliwe braki w przepisach dotyczących odpowiedniego stopnia ochrony i w razie konieczności formułując ewentualne zalecenia.

17. Zgodnie z art. 36 ust. 4 dyrektywy 2016/680 do Komisji Europejskiej należy monitorowanie na bieżąco zmian mogących wpłynąć na obowiązywanie decyzji stwierdzającej odpowiedni stopień ochrony.

18. Art. 36 ust. 3 dyrektywy 2016/680 stanowi, że okresowy przegląd musi odbywać się przynajmniej raz na cztery lata. Są to jednak ogólne ramy czasowe, które muszą zostać dostosowane do każdego państwa trzeciego lub organizacji międzynarodowej zgodnie z decyzją stwierdzającą odpowiedni stopień ochrony. W zależności od konkretnych okoliczności uzasadniony może być krótszy cykl przeglądu. Ponadto incydenty lub inne informacje na temat ram prawnych lub zmiany tych ram prawnych w danym państwie trzecim lub organizacji międzynarodowej mogą spowodować konieczność dokonania przeglądu przed planowanym terminem. Wydaje się również właściwe, aby pierwszy przegląd całkowicie nowej decyzji stwierdzającej odpowiedni stopień ochrony przeprowadzono dosyć szybko i stopniowo dostosowywano cykl przeglądu w zależności od wyniku.

19. Biorąc pod uwagę upoważnienie EROD do przekazywania Komisji Europejskiej opinii na temat tego, czy państwo trzecie, terytorium lub określony sektor lub określone sektory w tym państwie trzecim lub organizacja międzynarodowa nie zapewniają już odpowiedniego stopnia ochrony, EROD musi, w odpowiednim czasie, otrzymać istotne informacje dotyczące monitorowania przez Komisję Europejską istotnych zmian w tym państwie trzecim lub organizacji międzynarodowej. W związku z tym EROD powinna być na bieżąco informowana o każdym procesie przeglądu i misji przeglądowej w państwie trzecim lub organizacji międzynarodowej. EROD zaleca zapraszanie jej do udziału w tych procesach przeglądu i misjach, jak przewidziano w decyzji w sprawie Tarczy Prywatności i w decyzji stwierdzającej odpowiedni stopień ochrony w odniesieniu do Japonii.

20. Należy również zauważyć, że zgodnie z art. 36 ust. 5 dyrektywy 2016/680 Komisja Europejska ma prawo uchylić, zmienić lub zawiesić wydane decyzje stwierdzające odpowiedni stopień ochrony, jeżeli państwo trzecie lub organizacja międzynarodowa przestały zapewniać odpowiedni stopień ochrony. Procedura uchylenia, zmiany lub zawieszenia wymaga zwrócenia się do EROD o wydanie opinii zgodnie z art. 51 ust. 1 lit. g) dyrektywy 2016/680.

21. Ponadto , bez uszczerbku dla uprawnień organów prokuratorskich, organy nadzorcze powinny również mieć uprawnienie do wnoszenia naruszeń tej dyrektywy przed organy sądowe lub do udziału w postępowaniu sądowym[13]. W szczególności z wyroku Trybunału Sprawiedliwości Unii Europejskiej w sprawie Schrems I wynika, że organy ochrony danych muszą mieć możliwość wszczęcia postępowania sądowego przed sądami krajowymi, jeżeli uznają, że zarzuty danej osoby przeciwko decyzji stwierdzającej odpowiedni stopień ochrony są zasadne[14]. W wyroku w sprawie Schrems II potwierdzono tę ocenę[15].

4. UNIJNE NORMY DOTYCZĄCE ODPOWIEDNIEGO STOPNIA OCHRONY W ZAKRESIE WSPÓŁPRACY POLICYJNEJ I WSPÓŁPRACY WYMIARÓW SPRAWIEDLIWOŚCI W SPRAWACH KARNYCH

22. Co do istoty decyzje stwierdzające odpowiedni stopień ochrony powinny koncentrować się na ocenie obowiązującego prawodawstwa danego państwa trzeciego jako całości, w teorii i praktyce, w świetle kryteriów oceny określonych w art. 36 dyrektywy 2016/680. System państwa trzeciego lub organizacji międzynarodowej musi zawierać następujące podstawowe ogólne zasady i mechanizmy proceduralne w zakresie ochrony danych osobowych, jak również zasady i mechanizmy egzekwowania tej ochrony.

23. W art. 36 ust. 2 dyrektywy 2016/680 ustanowiono elementy, które Komisja Europejska uwzględnia podczas sprawdzania, czy stopień ochrony zapewniony w państwie trzecim lub organizacji międzynarodowej jest odpowiedni.

24. W szczególności Komisja bierze pod uwagę praworządność, poszanowanie praw człowieka i podstawowych wolności[16], odpowiednie przepisy, a także wdrażanie tych przepisów, skuteczne

prawem Unii była zapewniona w razie przekazywania danych osobowych z Unii do państwa trzeciego. Nawet jeżeli środki mające na celu zapewnienie takiego stopnia ochrony mogą różnić się od środków wprowadzonych w Unii w celu zagwarantowania poszanowania wymogów płynących z prawa Unii, to jednak środki te powinny w praktyce skutecznie zapewniać ochronę merytorycznie równoważną ochronie gwarantowanej w Unii".

[13] Zob. art. 47 ust. 5 dyrektywy 2016/680 i jej motyw 82.

[14] Zob. Schrems I, pkt 65: „W tym względzie do krajowego ustawodawcy należy ustanowienie drogi prawnej umożliwiającej krajowemu organowi nadzorczemu podniesienie zarzutów, które uważa on za zasadne, przed sądami krajowymi, po to, aby te ostatnie, jeśli podzielają wątpliwości tego organu co do ważności decyzji Komisji, wystąpiły z wnioskiem o wydanie orzeczenia w trybie prejudycjalnym w celu zbadania ważności tej decyzji".

[15] Zob. Schrems II, pkt 120: „nawet w przypadku wydania przez Komisję decyzji stwierdzającej odpowiedni stopień ochrony właściwy krajowy organ nadzorczy, do którego dana osoba wniosła skargę dotyczącą ochrony jej praw i wolności w związku z przetwarzaniem dotyczących jej danych osobowych, powinien mieć możliwość zbadania w sposób całkowicie niezależny tego, czy przekazywanie tych danych spełnia wymogi ustanowione w RODO oraz, w odpowiednim przypadku, wniesienia do sądów krajowych skargi mającej na celu skierowanie przez te sądy, jeśli podzielą one wątpliwości tego organu co do ważności tej decyzji stwierdzającej odpowiedni stopień ochrony, odesłania prejudycjalnego mającego doprowadzić do przeanalizowania tej ważności".

[16] Oceniając ramy prawne państwa trzeciego, należy wziąć pod uwagę możliwość nałożenia kary śmierci lub jakiejkolwiek innej formy okrutnego lub nieludzkiego traktowania na podstawie danych przekazywanych z UE. Gdyby taka kara lub takie traktowanie były przewidziane w prawie państwa trzeciego, w ramach prawnych

i egzekwowalne prawa osób, których dane dotyczą, oraz prawo osób, których dane osobowe są przekazywane, do skutecznych administracyjnych i sądowych środków zaskarżenia, istnienie i skuteczne funkcjonowanie co najmniej jednego niezależnego organu nadzorczego oraz zobowiązania międzynarodowe zaciągnięte przez państwo trzecie lub organizację międzynarodową.

25. Jasne jest zatem, że jakakolwiek konstruktywna analiza odpowiedniej ochrony musi obejmować dwa podstawowe elementy: treść mających zastosowanie przepisów oraz środki służące zapewnieniu ich skutecznego wdrożenia. Do Komisji Europejskiej należy regularne sprawdzanie, czy obowiązujące przepisy są skuteczne w praktyce.

26. Podstawowe ogólne zasady oraz wymogi proceduralne w zakresie ochrony danych i dotyczące egzekwowania tej ochrony, które można by postrzegać jako minimalny wymóg zapewnienia odpowiedniego stopnia ochrony, wynikają z Karty praw podstawowych UE i dyrektywy 2016/680. Przepisy ogólne dotyczące ochrony danych osobowych i prywatności w państwie trzecim nie są wystarczające. Wręcz przeciwnie ramy prawne państwa trzeciego lub organizacji międzynarodowej powinny obejmować przepisy szczególne określające w konkretny sposób prawo do ochrony danych osobowych w obszarze ścigania przestępstw. Państwo trzecie powinno dawać gwarancje zapewniające odpowiedni stopień ochrony, zasadniczo odpowiadający stopniowi przewidzianemu w Unii. Przepisy te muszą być możliwe do wyegzekwowania na drodze prawnej.

27. Ponadto w odniesieniu do zasady proporcjonalności[17] TSUE orzekł w odniesieniu do przepisów państw członkowskich, że kwestię, czy ograniczenie prawa do prywatności i ochrony danych może być uzasadnione, należy oceniać z jednej strony poprzez badanie **wagi ingerencji**, jaką stanowi takie ograniczenie[18], a z drugiej strony poprzez sprawdzenie, czy **znaczenie celu interesu ogólnego**, do którego zmierza to ograniczenie, jest proporcjonalne do tej wagi[19].

28. Zgodnie z orzecznictwem TSUE podstawa prawna umożliwiająca ingerencję w prawa podstawowe musi– aby spełniać wymóg proporcjonalności – sama określać zakres ograniczenia wykonywania danego prawa[20]. Odstępstwa od ochrony danych osobowych i jej ograniczenia mogą być stosowane jedynie wtedy, gdy jest to absolutnie konieczne[21]. Aby spełnić ten wymóg, oprócz określenia jasnych i precyzyjnych reguł dotyczących zakresu i stosowania rozpatrywanego środka, dane uregulowanie musi ustanawiać minimalne wymagania służące temu, aby osoby, których dane osobowe zostały przekazane, były zaopatrzone w wystarczające zabezpieczenia umożliwiające rzeczywistą ochronę ich danych przed ryzykiem nadużyć. „Powinno ono w szczególności wskazywać, w jakich okolicznościach i pod jakimi warunkami może zostać przyjęty środek przewidujący przetwarzanie takich danych, gwarantując w ten sposób, że

takiego państwa powinny znaleźć się dodatkowe zabezpieczenia gwarantujące, że dane przekazywane z UE nie będą wykorzystywane do żądania, orzekania lub wykonania kary śmierci ani do jakiejkolwiek innej formy okrutnego i nieludzkiego traktowania (np. umowa międzynarodowa nakładająca warunki przekazywania danych, zobowiązanie państwa trzeciego do nienakładania kary śmierci lub jakiejkolwiek innej formy okrutnego lub nieludzkiego traktowania na podstawie danych przekazywanych z UE lub moratorium na karę śmierci).

[17] Art. 52 ust. 1 karty.

[18] Sąd podkreślił na przykład, że „ingerencja, jaką stanowi gromadzenie w czasie rzeczywistym danych umożliwiających zlokalizowanie urządzeń końcowych, jest szczególnie poważna, ponieważ dane te umożliwiają właściwym organom krajowym dokładne i stałe monitorowanie przemieszczania się użytkowników telefonów komórkowych (...)" (sprawy połączone C-511/18, C-512/18 i C-520/18, La Quadrature du Net i in., wyrok z dnia 6 października 2020 r., ECLI:EU:C:2020:791, pkt 187 wraz z przytoczonym tam orzecznictwem).

[19] La Quadrature du Net i in., pkt 131.

[20] Schrems II, pkt 180.

[21] Schrems II, pkt 176 wraz z przytoczonym tam orzecznictwem.

ingerencja będzie ograniczona do tego, co ściśle konieczne. Konieczność zaopatrzenia w takie gwarancje jest istotna jeszcze bardziej wówczas, gdy dane osobowe są przetwarzane w sposób zautomatyzowany"[22].

29. EROD przyjęła zalecenia odzwierciedlające orzecznictwo TSUE i Europejskiego Trybunału Praw Człowieka (ETPC) w dziedzinie nadzoru określające niezbędne gwarancje, których należy szukać w prawie państwa trzeciego w ramach oceny ingerencji takich środków nadzoru państwa trzeciego w prawa osób, których dane dotyczą, w przypadku gdy dane są przekazywane temu państwu trzeciemu na mocy RODO[23]. EROD uważa, że aby ocenić, czy spełnione są warunki, o których mowa w art. 36 ust. 2 lit. a) dyrektywy 2016/680, przy ocenie, czy państwo trzecie zapewnia odpowiedni stopień ochrony w obszarze nadzoru zgodnie z tą dyrektywą, należy wziąć pod uwagę gwarancje określone w tych zaleceniach, mając na uwadze w tym kontekście dalsze szczegółowe warunki w obszarze nadzoru.

30. W odniesieniu do wymogu określonego w art. 36 ust. 2 lit. b) państwo trzecie powinno nie tylko zapewnić skuteczny niezależny nadzór nad ochroną danych, ale również zapewnić mechanizmy współpracy z organami ochrony danych państw członkowskich[24].

31. W odniesieniu do wymogu określonego w art. 36 ust. 2 lit. c) poza międzynarodowymi zobowiązaniami, które przyjęły państwo trzecie lub organizacja międzynarodowa, należy również wziąć pod uwagę obowiązki wynikające z udziału państwa trzeciego lub organizacji międzynarodowej w systemach wielostronnych lub regionalnych, zwłaszcza w odniesieniu do ochrony danych osobowych, a także realizację tych obowiązków; w szczególności należy wziąć pod uwagę przystąpienie państwa trzeciego do innych umów międzynarodowych o ochronie danych osobowych, np. do Konwencji Rady Europy z dnia 28 stycznia 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych oraz do Protokołu dodatkowego do tej konwencji (konwencja nr 108[25] i jej zaktualizowana wersja – konwencja nr 108+). Można również wziąć pod uwagę to, czy państwo trzecie przestrzega zasad zawartych w dokumentach międzynarodowych, takich jak wydany przez Radę Europy „Praktyczny przewodnik w sprawie wykorzystywania danych osobowych przez policję –sposoby ochrony danych osobowych podczas walki z przestępczością" (Practical Guide on the use of personal data in the police sector: how to protect personal data while combatting crime).

32. Decyzja stwierdzająca odpowiedni stopień ochrony powinna gwarantować, że dany zagraniczny system jako całość zapewnia wymagany stopień ochrony, biorąc pod uwagę istotę prawa do prywatności i prawa do ochrony danych oraz skuteczne wprowadzenie w życie tych praw, nadzór nad ich przestrzeganiem i ich egzekwowanie, w tym w odniesieniu do danych przekazywanych do tego państwa trzeciego. Jak podkreślił TSUE w wyroku w sprawie Schrems II, wysoki stopień ochrony należy zapewnić również w sytuacji, gdy dane są przekazywane do państwa trzeciego[26].

33. Ponadto przy przyjmowaniu decyzji stwierdzających odpowiedni stopień ochrony w odniesieniu jedynie do konkretnego terytorium lub określonego sektora w państwie trzecim Komisja powinna wziąć pod uwagę jasne i obiektywne kryteria, na przykład odnoszące się do konkretnych czynności

[22] Schrems II, pkt 176 wraz z przytoczonym tam orzecznictwem.

[23] Zalecenia EROD 02/2020 dotyczące niezbędnych gwarancji europejskich dla środków nadzoru, przyjęte w dniu 10 listopada 2020 r.

[24] Motyw 67 dyrektywy 2016/680.

[25] Motyw 68 dyrektywy 2016/680.

[26] Zob. pkt 93.

przetwarzania lub zakresu właściwych norm prawnych i ustawodawstwa obowiązującego w państwie trzecim[27].

A. Zasady ogólne i zabezpieczenia

a) Pojęcia

34. W danym systemie prawnym powinny istnieć podstawowe pojęcia dotyczące ochrony danych osobowych. Nie muszą one odzwierciedlać terminologii dyrektywy 2016/680, ale powinny odzwierciedlać pojęcia zawarte w europejskim prawie w dziedzinie ochrony danych i być z nimi spójne. Przykładowo dyrektywa 2016/680 zawiera następujące istotne pojęcia: „dane osobowe", „przetwarzanie danych osobowych", „właściwe organy", „administrator danych", „podmiot przetwarzający dane", „odbiorca", „dane wrażliwe", „prawidłowość", „profilowanie", „uwzględnienie ochrony danych w fazie projektowania i domyślna ochrona danych", „organ nadzorczy" i „pseudonimizacja".

b) Zgodność z prawem i rzetelność przetwarzania danych osobowych (art. 4 – motyw 26)

35. Zgodnie z art. 8 ust. 2 karty dane osobowe powinny w szczególności być przetwarzane „w określonych celach i za zgodą osoby zainteresowanej lub na innej uzasadnionej podstawie przewidzianej ustawą"[28]. W kontekście ścigania przestępstw należy jednak zauważyć, że wykonywanie zadań polegających na zapobieganiu przestępczości, prowadzeniu postępowań przygotowawczych, wykrywaniu i ściganiu czynów zabronionych, instytucjonalnie powierzonych na mocy prawa właściwym organom, pozwala tym organom wymagać lub nakazywać, aby osoby fizyczne zastosowały się do stawianych żądań. W takim przypadku zgoda osoby, której dane dotyczą, nie powinna stanowić podstawy prawnej przetwarzania danych osobowych przez właściwe organy[29].

36. Ta podstawa prawna powinna określać jasne i precyzyjne reguły dotyczące zakresu i stosowania odpowiednich czynności przetwarzania danych oraz ustanawiać minimalne zabezpieczenia[30]. Ponadto TSUE przypomniał, że „to uregulowanie musi być prawnie wiążące w prawie wewnętrznym"[31].

37. Aby przetwarzanie danych[32] było zgodne z prawem, powinno ono być niezbędne do wykonania zadania realizowanego przez właściwy organ do celów zapobiegania przestępczości, prowadzenia

[27] Motyw 67 dyrektywy 2016/680.
[28] Zob. Schrems II, pkt 173.
[29] Motyw 35 dyrektywy 2016/680 stanowi również, że „[j]eżeli osoba, której dane dotyczą, musi wywiązać się z obowiązku prawnego, nie ma ona faktycznego, swobodnego wyboru, a tym samym nie można uznać, iż jej reakcja jest swobodnym wyrazem jej woli. Nie powinno to stanowić dla państw członkowskich przeszkody w ustanowieniu z mocy prawa, że osoba, której dane dotyczą, może wyrazić zgodę na przetwarzanie jej danych osobowych do celów określonych w niniejszej dyrektywie, takich jak badania DNA w postępowaniu przygotowawczym czy monitorowanie miejsca jej pobytu za pomocą aparatury elektronicznej na potrzeby wykonania kary".
[30] Zob. Schrems II, pkt 175 i 180 oraz opinia 1/15, pkt 139 i przytoczone tam orzecznictwo.
[31] Zob. sprawa C-623/17, Privacy International przeciwko Secretary of State for Foreign and Commonwealth Affairs i in., wyrok z dnia 6 października 2020 r., ECLI:EU:C:2020:790, pkt 68. Należy również wyjaśnić, że we francuskiej wersji wyroku TSUE posługuje się terminem „réglementation", którego znaczenie jest szersze i obejmuje nie tylko akty Parlamentu.
[32] Przetwarzanie danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz przetwarzanie w sposób inny niż zautomatyzowany danych osobowych stanowiących lub mających stanowić część zbioru danych.

postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom[33]. Cele te powinny być określone w prawie krajowym.

38. Dane osobowe są przetwarzane rzetelnie. Zasada rzetelnego przetwarzania obowiązująca w ochronie danych jest pojęciem odrębnym względem prawa do rzetelnego procesu, które jest zdefiniowane w art. 47 karty i w art. 6 europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności („EKPC")[34].

c) Zasada ograniczenia celu (art. 4)

39. Konkretne cele przetwarzania danych osobowych powinny być wyraźne, uzasadnione i określone w momencie zbierania tych danych[35].

40. Dane powinny być przetwarzane w konkretnym, wyraźnym i prawnie uzasadnionym celu, mieszczącym się w ramach celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar[36], w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom w państwie trzecim, a następnie wykorzystywane do któregokolwiek z tych celów, o ile nie jest to niezgodne z pierwotnym celem przetwarzania danych (np. do celów toczących się równolegle postępowań egzekucyjnych lub archiwizacji w interesie publicznym, wykorzystania danych przetwarzanych w powyższych celach do celów naukowych, statystycznych lub historycznych) oraz z zastrzeżeniem stosowania odpowiednich zabezpieczeń chroniących prawa i wolności osób, których dane dotyczą. Jeżeli dane osobowe przetwarza ten sam lub inny administrator (właściwy organ[37]) w celu zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, innym niż cel, w którym dane zostały zebrane, przetwarzanie takie powinno być dopuszczalne, pod warunkiem że przetwarzanie jest dozwolone na podstawie właściwych przepisów prawa oraz jest niezbędne i proporcjonalne do tego innego celu[38]. Należy także wziąć pod uwagę istnienie mechanizmu informowania odpowiednich właściwych organów państw członkowskich o takim dalszym przetwarzaniu danych[39]. Ponadto nie należy w żadnym wypadku obniżać stopnia ochrony osób fizycznych przewidzianego w Unii w dyrektywie 2016/680, także w przypadkach, gdy dane osobowe są przekazywane z państwa trzeciego administratorom lub podmiotom przetwarzającym w tym samym państwie trzecim[40].

[33] Właściwymi organami są wszelkie organy publiczne właściwe do takich celów oraz wszelkie inne organy lub podmioty, którym prawo powierza wykonywanie władzy publicznej i uprawnień publicznych w tym celu.
[34] Motyw 26 dyrektywy 2016/680.
[35] Motyw 26 dyrektywy 2016/680.
[36] Cele te obejmują „czynności policji podejmowane, gdy nie wiadomo, czy dane zdarzenie jest czynem zabronionym. Czynności te mogą też polegać na sprawowaniu władzy poprzez stosowanie środków przymusu takich jak czynności policji podczas demonstracji, dużych imprez sportowych czy zamieszek. Czynności te obejmują również utrzymywanie prawa i porządku jako zadanie powierzone policji lub innym organom ścigania, gdy jest to konieczne do ochrony przed zagrożeniami dla bezpieczeństwa publicznego i dla prawnie chronionych podstawowych interesów społecznych i do zapobiegania takim zagrożeniom, które mogą prowadzić do popełnienia czynu zabronionego" (motyw 12 dyrektywy 2016/680). Należy je odróżnić od celu związanego z bezpieczeństwem narodowym i od czynności, które wchodzą w zakres stosowania tytułu V rozdział 2 Traktatu o Unii Europejskiej (TUE) (motyw 14 dyrektywy 2016/680).
[37] Zob. przypis 33.
[38] Motyw 29 dyrektywy 2016/680.
[39] Takim mechanizmem mogłyby być na przykład wspólnie uzgodnione kodeksy postępowania, obowiązek powiadamiania odpowiednich organów na mocy instrumentu międzynarodowego, w tym ewentualne powiadomienia automatyczne, lub inne podobne środki zapewniające przejrzystość.
[40] Motyw 64 dyrektywy 2016/680.

d) Szczególne warunki dalszego przetwarzania do innych celów (art. 9)

41. Jeżeli chodzi o dalsze przetwarzanie lub ujawnianie danych przekazywanych z UE do celów innych niż ściganie przestępstw, takich jak cele związane z bezpieczeństwem narodowym, powinno ono być również przewidziane prawem, niezbędne i proporcjonalne. Należy także wziąć pod uwagę istnienie mechanizmu informowania odpowiednich właściwych organów państw członkowskich o takim dalszym przetwarzaniu danych[41]. Również w tym przypadku, po dalszym przetworzeniu lub ujawnieniu, dane powinny być objęte takim samym stopniem ochrony, jakim były objęte, gdy były pierwotnie przetwarzane przez właściwy organ odbierający dane.

e) Zasada minimalizacji danych

42. Dane powinny być adekwatne, stosowne i niewykraczające poza cele, w których są przetwarzane. W szczególności należy wziąć pod uwagę zastosowanie wymogów dotyczących uwzględniania ochrony danych w fazie projektowania oraz domyślnej ochrony danych, takich jak ograniczenia pól wprowadzania danych (ustrukturyzowane przekazywanie danych) lub zautomatyzowane i niezautomatyzowane kontrole jakości.

f) Zasada prawidłowości danych

43. Dane powinny być prawidłowe i w razie potrzeby uaktualniane. Zasadę prawidłowości danych należy jednak stosować z uwzględnieniem charakteru i celu przetwarzania. W szczególności w postępowaniu sądowym oświadczenia zawierające dane osobowe opierają się na subiektywnym osądzie osób fizycznych i nie zawsze są weryfikowalne. Dlatego wymóg prawidłowości danych nie powinien odnosić się do prawidłowości oświadczenia, lecz jedynie do faktu, że konkretne oświadczenie zostało złożone[42].

44. Należy zapewnić, aby nieprawidłowe, niekompletne lub nieaktualne dane osobowe nie były przesyłane ani udostępniane[43] oraz aby przewidziane były procedury korygowania lub usuwania nieprawidłowych danych. W szczególności należy wziąć pod uwagę wszelkie systemy klasyfikacji przetwarzanych informacji, wiarygodność źródła i stopień weryfikacji faktów[44].

g) Zasada zatrzymywania danych

45. Dane nie powinny być przechowywane przez okres dłuższy, niż jest to niezbędne do celów, w których są przetwarzane. Należy ustanowić odpowiednie mechanizmy usuwania danych osobowych; może to być określony termin lub okresowy przegląd konieczności przechowywania danych osobowych (lub połączenie obu tych metod – określenie maksymalnego czasu przechowywania i przeprowadzanie okresowego przeglądu w wyznaczonych odstępach czasu)[45]. Dane osobowe przechowywane przez dłuższy okres w celu archiwizacji w interesie publicznym, wykorzystania do celów naukowych, statystycznych lub historycznych powinny podlegać odpowiednim zabezpieczeniom (np. dotyczącym dostępu)[46].

[41] Zob. przypis 39.
[42] Motyw 30 dyrektywy 2016/680.
[43] Motyw 32 dyrektywy 2016/680.
[44] Np. system oceny 4x4 dla ocen wiarygodności i kodeksów postępowania.
[45] Art. 5 dyrektywy 2016/680.
[46] Motyw 26 dyrektywy 2016/680.

h) Zasada bezpieczeństwa i poufności (art. 29, motywy 28 i 71)

46. Podmiot przetwarzający dane osobowe powinien zapewnić przetwarzanie danych w sposób zapewniający im bezpieczeństwo, w tym ochronę przed nieuprawnionym dostępem do nich i do sprzętu służącego ich przetwarzaniu oraz przed nieuprawnionym korzystaniem z tych danych i z tego sprzętu. Obejmuje to ochronę przed przetwarzaniem niezgodnym z prawem, a także przed przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych i organizacyjnych oraz odpowiednie środki służące zaradzeniu tym zjawiskom. Przy określaniu poziomu bezpieczeństwa należy uwzględnić stan wiedzy technicznej, koszty wdrożenia oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze.

47. Należy zapewnić bezpieczne kanały komunikacji między organami państw członkowskich przekazującymi dane osobowe a organami państw trzecich, które je otrzymują.

i) Zasada przejrzystości (art. 13, motywy 26, 39, 42, 43, 44, 46)

48. Osobom fizycznym należy uświadomić ryzyko, zasady, zabezpieczenia i prawa związane z przetwarzaniem ich danych osobowych oraz sposoby wykonywania praw przysługujących im w związku z takim przetwarzaniem[47].

49. Osobom fizycznym powinny być udostępniane informacje na temat najważniejszych elementów przetwarzania ich danych osobowych. Informacje te powinny być łatwo dostępne i zrozumiałe, napisane przy użyciu jasnego i prostego języka. Powinny one obejmować cel przetwarzania danych, tożsamość administratora danych, przyznane mu prawa[48] oraz inne informacje w zakresie, w jakim jest to niezbędne do zapewnienia rzetelności.

50. Mogą istnieć pewne wyjątki od tego prawa do informacji. Ograniczenie takie powinno być jednak dozwolone na podstawie aktu prawnego, a także powinno być niezbędne i proporcjonalne, aby uniknąć utrudniania prowadzenia urzędowych lub sądowych dochodzeń, postępowań przygotowawczych lub procedur, aby uniknąć uniemożliwienia zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, aby chronić bezpieczeństwo publiczne i narodowe oraz aby chronić prawa i wolności innych osób, o ile takie częściowe lub całkowite ograniczenie stanowi niezbędny i proporcjonalny środek w społeczeństwie demokratycznym, przy należytym uwzględnieniu praw podstawowych i uzasadnionych interesów danej osoby fizycznej. Takie ograniczenia należy również rozważyć i ocenić z uwzględnieniem możliwości złożenia skargi do organu nadzorczego lub skorzystania ze środka ochrony prawnej. W każdym razie wszelkie ewentualne ograniczenia powinny mieć charakter tymczasowy, a nie ogólny, oraz powinny być objęte podobnymi warunkami, zabezpieczeniami i ograniczeniami do tych, jakie są wymagane na mocy Karty praw podstawowych Unii Europejskiej i EKPC, zgodnie z wykładnią zawartą odpowiednio w orzecznictwie TSUE i ETPC, a w szczególności szanować istotę tych praw i wolności.

j) Prawo dostępu, prawo do sprostowania i usunięcia danych (art. 14 i 16)

51. Osoba, której dane dotyczą, powinna mieć prawo do uzyskania potwierdzenia, czy przetwarzane są dane jej dotyczące, a jeżeli takie dane są przetwarzane, powinna mieć prawo dostępu do swoich danych. Prawo to powinno obejmować co najmniej pewne informacje na temat

[47] Motyw 26 dyrektywy 2016/680.
[48] Zarówno prawa materialne (prawo dostępu, prawo do sprostowania itp.), jak i prawo do dochodzenia roszczeń.

przetwarzania, takie jak cele i podstawa prawna przetwarzania, informacje o prawie wniesienia skargi do organu nadzorczego oraz kategorie odnośnych danych osobowych[49]. Jest to szczególnie ważne w przypadku, gdy przejrzystość osiąga się za pomocą ogólnego zawiadomienia (np. informacji na stronie internetowej organu).

52. Osoba, której dane dotyczą, powinna mieć prawo do sprostowania swoich danych z określonych powodów, na przykład jeżeli okaże się, że są one nieprawidłowe lub niekompletne. Osoba, której dane dotyczą, powinna mieć również prawo do usunięcia swoich danych, na przykład gdy ich przetwarzanie nie jest już niezbędne lub jest niezgodne z prawem.

53. Wykonanie tych praw nie powinno być nadmiernie uciążliwe dla osoby, której dane dotyczą.

k) Ograniczenia praw osoby, której dane dotyczą

54. Ewentualne ograniczenia tych praw mogłyby zostać ustanowione, aby uniknąć utrudniania prowadzenia urzędowych lub sądowych dochodzeń, postępowań przygotowawczych lub procedur, aby uniknąć uniemożliwienia zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, aby chronić bezpieczeństwo publiczne i narodowe oraz aby chronić prawa i wolności innych osób, o ile takie częściowe lub całkowite ograniczenie stanowi niezbędny i proporcjonalny środek w społeczeństwie demokratycznym, przy należytym uwzględnieniu praw podstawowych i uzasadnionych interesów danej osoby fizycznej. Takie ograniczenia należy również rozważyć i ocenić z uwzględnieniem możliwości złożenia skargi do organu nadzorczego lub skorzystania z sądowego środka zaskarżenia.

l) Ograniczenie dalszego przekazywania danych (art. 35, motywy 64–65)

55. W przypadku dalszego przekazywania danych osobowych przez pierwotnego odbiorcę do innego państwa trzeciego lub organizacji międzynarodowej nie należy obniżać przewidzianego w Unii stopnia ochrony danych osób fizycznych, których dane są przekazywane. W związku z tym takie dalsze przekazywanie danych powinno być dozwolone wyłącznie w przypadku zapewnienia ciągłości poziomu ochrony przyznanego prawem Unii[50]. W szczególności dalszy odbiorca (tj. odbiorca dalszego przekazywania) powinien być organem właściwym do celów ścigania przestępstw[51], a dalsze przekazywanie danych może odbywać się wyłącznie w ograniczonych i określonych celach i o ile istnieje podstawa prawna do takiego przetwarzania.

56. Należy również wziąć pod uwagę istnienie mechanizmu, w ramach którego właściwe organy danego państwa członkowskiego są informowane o dalszym przekazywaniu danych oraz wyrażają na nie zgodę. Pierwotny odbiorca danych przekazywanych z UE powinien ponosić odpowiedzialność za to, by odpowiedni właściwy organ państwa członkowskiego zezwolił na dalsze przekazywanie danych[52] oraz by zapewniono odpowiednie zabezpieczenia dla przekazywanych danych w przypadku braku decyzji stwierdzającej odpowiedni stopień ochrony w odniesieniu do państwa trzeciego, do którego dane byłyby dalej przekazywane[53], a ponadto

[49] Art. 14 dyrektywy 2016/680.
[50] Zob. również opinia 1/15.
[51] Zob. przypis 33.
[52] W tym kontekście należy uwzględnić istnienie obowiązku lub zobowiązania do wdrożenia odpowiednich kodeksów postępowania określonych przez organy państw członkowskich przekazujące dane.
[53] Powyższe wymogi nie naruszają szczególnych warunków dalszego przekazywania danych do odpowiedniego państwa określonych w dyrektywie 2016/680 (art. 35 ust. 1 lit. c) i e)).

pierwotny odbiorca danych powinien być w stanie udowodnić, że właściwy organ państwa członkowskiego udzielił takiej zgody oraz że zapewniono takie zabezpieczenia.

m) Zasada rozliczalności (art. 4 ust. 4)

57. Administrator powinien odpowiadać za przestrzeganie zasad ochrony danych określonych w art. 4 dyrektywy 2016/680 i być w stanie wykazać ich przestrzeganie.

B. Przykłady dodatkowych zasad, które mają być stosowane do konkretnych rodzajów przetwarzania

a) Szczególne kategorie danych (art. 10 i motyw 37)

58. Jeżeli przetwarzanie obejmuje „szczególne kategorie danych", powinny istnieć szczególne zabezpieczenia[54] służące ochronie przed szczególnymi rodzajami ryzyka[55]. Kategorie te powinny odzwierciedlać kategorie określone w art. 10 dyrektywy 2016/680. Przetwarzanie danych należących do szczególnych kategorii powinno zatem podlegać szczególnym zabezpieczeniom i być dozwolone wyłącznie wtedy, jeżeli jest absolutnie niezbędne, pod pewnymi warunkami, na przykład w celu ochrony żywotnych interesów danej osoby.

b) Zautomatyzowane podejmowanie decyzji i profilowanie (art. 11 i motyw 38)

59. Decyzje oparte wyłącznie na zautomatyzowanym przetwarzaniu (zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach), w tym profilowaniu, które wywołują negatywne skutki prawne lub istotnie wpływają na osobę, której dane dotyczą, powinny być podejmowane jedynie pod pewnymi warunkami określonymi w ramach prawnych państwa trzeciego[56].

60. W systemie prawnym Unii Europejskiej takie warunki obejmują na przykład udzielenie konkretnych informacji osobie, której dane dotyczą, i prawo do uzyskania interwencji ludzkiej ze strony administratora, a zwłaszcza prawo do wyrażenia własnego stanowiska, uzyskania wyjaśnienia decyzji wydanej wskutek takiej analizy lub zaskarżenia tej decyzji.

61. Prawo państwa trzeciego powinno w każdym przypadku przewidywać niezbędne zabezpieczenia praw i wolności osób, których dane dotyczą. W związku z tym należy również wziąć pod uwagę istnienie mechanizmu informowania właściwych organów danego państwa członkowskiego o dalszym przetwarzaniu, takim jak wykorzystywanie przekazanych danych do profilowania na dużą skalę.

c) Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych (art. 20)

62. Oceniając odpowiedni stopień ochrony, należy zwrócić uwagę na istnienie obowiązku przyjmowania przez administratorów wewnętrznych polityk i wdrażania środków, które są zgodne z zasadami ochrony danych w fazie projektowania i domyślnej ochrony danych, z uwzględnieniem stanu wiedzy technicznej, kosztu wdrożenia i charakteru, zakresu, kontekstu i celów przetwarzania oraz ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia wynikające z przetwarzania – zarówno w czasie określania sposobów przetwarzania, jak i w czasie samego przetwarzania – oraz obowiązku przyjmowania przez administratorów odpowiednich środków technicznych i organizacyjnych, takich jak pseudonimizacja, zaprojektowanych w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń.

[54] Takie szczególne kategorie zostały również określone jako „dane wrażliwe" w motywie 37 dyrektywy 2016/680.
[55] Takimi dodatkowymi zabezpieczeniami mogą być np. szczególne środki bezpieczeństwa, ograniczone prawa dostępu dla pracowników, ograniczenia dotyczące dalszego przetwarzania, zautomatyzowanego podejmowania decyzji, dalszego udostępniania lub dalszego przekazywania danych.
[56] Opinia 1/15, pkt 173.

C. Mechanizmy proceduralne i mechanizmy egzekwowania prawa

63. Mimo że środki, z których korzysta państwo trzecie w celu zapewnienia odpowiedniego stopnia ochrony, mogą się różnić od środków stosowanych w Unii Europejskiej[57], system zgodny z systemem europejskim musi zawierać następujące elementy:

a) Właściwy niezależny organ nadzorczy (art. 36 ust. 2 lit. b), art. 36 ust. 3 i motyw 67)

64. Powinien istnieć co najmniej jeden niezależny organ nadzorczy odpowiedzialny za zapewnianie i egzekwowanie przestrzegania przepisów o ochronie danych osobowych i prywatności w państwie trzecim. Podczas wypełniania swoich zadań i wykonywania swoich uprawnień organ nadzorczy powinien działać w sposób w pełni niezależny i bezstronny, a w trakcie tych działań nie powinien zwracać się o żadne instrukcje ani takich instrukcji przyjmować. W tym kontekście organ nadzorczy powinien dysponować wszelkimi odpowiednimi uprawnieniami do egzekwowania skutecznego przestrzegania przepisów dotyczących ochrony danych osobowych i propagowania wiedzy na ten temat. Należy również rozważyć personel i budżet organu nadzorczego. Organ nadzorczy powinien być też w stanie prowadzić dochodzenia z urzędu. Jego zadaniem powinno być również udzielanie pomocy i doradzanie osobom, których dane dotyczą, w zakresie wykonywania przysługujących im praw (zob. również lit. c) poniżej). W decyzjach stwierdzających odpowiedni stopień ochrony należy określić, w stosownych przypadkach, ten organ nadzorczy lub te organy nadzorcze oraz mechanizmy współpracy z organami nadzorczymi państw członkowskich w celu egzekwowania przepisów o ochronie danych.

b) Skuteczne wdrażanie przepisów dotyczących ochrony danych

65. System państwa trzeciego powinien zapewniać wysoki stopień świadomości wśród administratorów danych oraz podmiotów przetwarzających dane osobowe w ich imieniu w zakresie ich obowiązków, zadań i zakresu odpowiedzialności oraz wśród osób, których dane dotyczą, w zakresie ich praw i sposobów wykonywania tych praw. Istnienie skutecznych i zniechęcających sankcji może odegrać ważną rolę w zapewnieniu poszanowania przepisów, podobnie jak sprawić to mogą systemy bezpośredniej weryfikacji przez organy, audytorów lub niezależnych inspektorów ochrony danych.

66. Ramy ochrony danych osobowych obowiązujące w państwie trzecim powinny zobowiązywać administratorów danych lub podmioty przetwarzające dane osobowe w ich imieniu do przestrzegania tych ram oraz nakładać na nich obowiązek, by byli w stanie wykazać zgodność z ramami, w szczególności właściwemu organowi nadzorczemu. Tego rodzaju środki powinny obejmować prowadzenie rejestrów lub dzienników czynności przetwarzania danych przez odpowiedni okres. Mogą one również obejmować na przykład oceny skutków dla ochrony danych, wyznaczenie inspektora ochrony danych lub uwzględnienie ochrony danych w fazie projektowania i domyślną ochronę danych.

c) System ochrony danych ułatwia wykonywanie praw osobie, której dane dotyczą (art. 12, 17 i 46 dyrektywy 2016/680)

67. Ramy ochrony danych obowiązujące w państwie trzecim powinny zobowiązywać administratorów danych do ułatwiania osobom, których dane dotyczą, wykonywania praw, o których mowa w sekcji A lit. j) powyżej, oraz powinny przewidywać, że organ nadzorczy w tym

[57] Schrems I, pkt 74.

państwie trzecim informuje na wniosek każdą osobę, której dane dotyczą, o wykonywaniu przysługujących jej praw[58].

d) System ochrony danych zapewnia odpowiednie mechanizmy dochodzenia roszczeń

68. Chociaż obecnie brak jest orzecznictwa dotyczącego odpowiedniego stopnia ochrony danych w systemie prawnym państwa trzeciego w rozumieniu dyrektywy 2016/680, TSUE dokonał wykładni podstawowego prawa do skutecznej ochrony sądowej przewidzianego w art. 47 Karty praw podstawowych Unii Europejskiej. Art. 47 akapit pierwszy karty stanowi, że każdy, kogo prawa i wolności zagwarantowane przez prawo Unii zostały naruszone, ma prawo do skutecznego środka prawnego przed sądem[59], zgodnie z warunkami przewidzianymi w tym artykule.

69. Zgodnie z utrwalonym orzecznictwem TSUE samo istnienie skutecznej kontroli sądowej służącej zapewnieniu poszanowania przepisów prawa Unii jest nierozerwalnie związane z istnieniem praworządności. Tak więc uregulowanie nieprzewidujące dla jednostek żadnej drogi prawnej pozwalającej na uzyskanie dostępu do dotyczących ich danych osobowych lub sprostowanie czy usunięcie takich danych nie zapewnia poszanowania zasadniczej istoty prawa podstawowego do skutecznej ochrony prawnej, wynikającego z art. 47 karty[60].

70. Osoba fizyczna powinna mieć możliwość skorzystania ze środków ochrony prawnej w celu szybkiego i skutecznego egzekwowania swoich praw, bez nadmiernych kosztów oraz w celu zapewnienia przestrzegania tych praw.

71. W związku z tym muszą istnieć mechanizmy nadzoru pozwalające na niezależne rozpatrywanie skarg oraz umożliwiające identyfikowanie w praktyce wszelkich naruszeń prawa do ochrony danych osobowych i poszanowania życia prywatnego oraz nakładanie kar za takie naruszenia.

72. W przypadku nieprzestrzegania przepisów osobie, której dane są przekazywane do państwa trzeciego, należy także zapewnić skuteczne administracyjne i sądowe środki zaskarżenia w państwie trzecim, w tym odszkodowanie z tytułu szkód poniesionych w wyniku niezgodnego z prawem przetwarzania jej danych osobowych. Jest to najważniejszy element, który wiąże się z systemem niezależnego orzekania lub arbitrażu, umożliwiający wypłatę odszkodowania i, w stosownych przypadkach, nałożenie sankcji.

[58] Wykonywanie praw osób, których dane dotyczą, może mieć charakter bezpośredni lub pośredni.
[59] TSUE jest zdania, że skuteczna ochrona sądowa może być zapewniona nie tylko przez sąd, ale również przez organ, który oferuje zabezpieczenia merytorycznie równoważne tym wymaganym w art. 47 karty (zob. Schrems II, pkt 197). Może to być istotne w szczególności dla organizacji międzynarodowych.
[60] Schrems II, pkt 187 i 194 wraz z przytoczonym tam orzecznictwem.



Zalecenia 02/2020 dotyczące niezbędnych gwarancji europejskich dla środków nadzoru

Przyjęte 10 listopada 2020 r.

Spis treści

1. WPROWADZENIE 4
2. INGERENCJE W PRAWA PODSTAWOWE 6
3. NIEZBĘDNE GWARANCJE EUROPEJSKIE 8
Gwarancja A - Przetwarzanie powinno opierać się na jasnych, precyzyjnych i dostępnych zasadach 9
Gwarancja B - Należy wykazać konieczność i proporcjonalność w odniesieniu do zgodnych z prawem zamierzonych celów 10
Gwarancja C - Mechanizm niezależnego nadzoru 12
Gwarancja D - Skuteczne środki ochrony prawnej muszą być dostępne dla osób fizycznych 13
4. UWAGI KOŃCOWE ..... **Error! Bookmark not defined.**

Europejska Rada Ochrony Danych (EROD)

uwzględniając art. 70 ust. 1 lit. e) rozporządzenia Parlamentu Europejskiego i Rady 2016/679/UE z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (zwanego dalej „RODO")[1],

uwzględniając Porozumienie EOG, a w szczególności jego załącznik XI i protokół 37, w brzmieniu zmienionym decyzją Wspólnego Komitetu EOG nr 154/2018 z dnia 6 lipca 2018 r.[2],

uwzględniając art.12 i 22 swojego regulaminu wewnętrznego,

uwzględniając dokument roboczy Grupy Roboczej Art. 29 w sprawie uzasadnienia ingerencji w podstawowe prawa do prywatności i ochrony danych poprzez środki nadzoru przy przekazywaniu danych osobowych (niezbędne gwarancje europejskie, zwane dalej „PGE"), WP237,

PRZYJĘŁA NASTĘPUJĄCE ZALECENIA

1. WPROWADZENIE

1. W następstwie wyroku w sprawie Schrems I organy ochrony danych UE, zgromadzone w Grupie Roboczej Art. 29, bazując na orzecznictwie, określiły niezbędne gwarancje europejskie, których należy przestrzegać, aby zagwarantować, że ograniczenia prawa do prywatności i ochrony danych osobowych przez środki nadzoru przy przekazywaniu danych osobowych, nie wykraczają poza to, co jest niezbędne i proporcjonalne w społeczeństwie demokratycznym.

2. EROD pragnie podkreślić, że niezbędne gwarancje europejskie oparte są na orzecznictwie Trybunału Sprawiedliwości Unii Europejskiej (zwanego dalej „TSUE") w odniesieniu do art. 7, 8, 47 i 52 Karty praw podstawowych UE (zwanej dalej „Kartą") oraz, w zależności od przypadku, w orzecznictwie Europejskiego Trybunału Praw Człowieka (zwanego dalej „ETPC") w odniesieniu do art. 8 europejskiej konwencji praw człowieka (zwanej dalej: „EKPC"), w którym poruszano kwestię nadzoru w państwach będących stronami EKPC[3].

[1] Niniejszy dokument nie odnosi się do przypadków przekazywania lub dalszego przekazywania, objętych zakresem dyrektywy (UE) 2016/680.
[2] Odniesienia do „państw członkowskich" w niniejszym dokumencie należy rozumieć jako odniesienia do „państw członkowskich EOG".
[3] W niniejszych zaleceniach termin „prawa podstawowe" pochodzi z Karty praw podstawowych UE. Obejmuje on jednak również „prawa człowieka", zawarte w europejskiej konwencji praw człowieka.

3. Aktualizacja niniejszego dokumentu ma na celu dalszy rozwój niezbędnych gwarancji europejskich, które pierwotnie opracowano w odpowiedzi na wyrok w sprawie Schrems I[4], w celu uwzględnienia wyjaśnień TSUE (i ETPC) od czasu jego pierwszej publikacji, w szczególności w przełomowym wyroku w sprawie Schrems II[5].

4. W swoim wyroku w sprawie Schrems II TSUE stwierdził, że przeprowadzone w świetle art. 7, 8 i 47 Karty badanie decyzji Komisji 2010/87/UE w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych podmiotom przetwarzającym mającym siedzibę w państwach trzecich nie doprowadziło do żadnych ustaleń, które mogłyby mieć wpływ na ważność tej decyzji, jakkolwiek unieważniło decyzję w sprawie Tarczy Prywatności. TSUE uznał, że decyzja w sprawie Tarczy Prywatności jest niezgodna z art. 45 ust. 1 RODO w świetle z art. 7, 8 i 47 Karty. Wyrok może zatem posłużyć za przykład sytuacji, gdy środki nadzoru w państwie trzecim (w tym przypadku był to art. 702 FISA i rozporządzenie wykonawcze nr 12 333 w Stanach Zjednoczonych) nie są dostatecznie ograniczone, zaś osoby, których dane dotyczą, nie mają dostępu do skutecznych środków ochrony prawnej w celu wykonania praw, zgodnie z wymogami prawa UE, co uniemożliwia uznanie stopnia ochrony w państwie trzecim za „merytorycznie równoważny" temu gwarantowanemu w Unii Europejskiej w rozumieniu z art. 45 ust. 1 RODO.

5. Powody unieważnienia decyzji w sprawie Tarczy Prywatności znajdują również zastosowanie do innych narzędzi przekazywania[6]. Jakkolwiek Trybunał dokonał wykładni art. 46 ust. 1 RODO w kontekście ważności standardowych klauzul umownych, to taka wykładnia ma zastosowanie do wszelkich przypadków przekazywania do państw trzecich w oparciu o jakiekolwiek narzędzie, o którym mowa w art. 46 RODO.[7]

6. Ostatecznie to do TSUE należy ocena, czy ingerencja w prawo podstawowe może być uzasadniona. Jednak w przypadku braku takiego orzeczenia i przy zastosowaniu obowiązującego orzecznictwa organy ochrony danych są zobowiązane do oceny indywidualnych przypadków, albo z urzędu albo w następstwie skargi, oraz do skierowania sprawy do sądu krajowego, jeżeli podejrzewają one, że przekazanie nie jest zgodne z art. 45, w przypadku decyzji stwierdzającej odpowiedni stopień ochrony, albo do zawieszenia lub zakazania przekazania, jeżeli uznają, że nie można zastosować art. 46 RODO, a ochrona przekazywanych danych wymagana na mocy prawa UE nie może zostać zapewniona za pomocą innych środków.

7. Celem zaktualizowanych niezbędnych gwarancji europejskich jest zapewnienie elementów pozwalających na zbadanie, czy środki nadzoru umożliwiające organom publicznym w państwie trzecim, tj. agencjom odpowiedzialnym za bezpieczeństwo narodowe lub organom ścigania, dostęp do danych osobowych można uznać za uzasadnioną ingerencję, czy też nie.

[4] Wyrok TSUE z dnia 6 października 2015 r., Maximillian Schrems przeciwko Data Protection Commissioner, sprawa C-362/14, UE:C:2015:650 (zwana dalej: „Schrems I").
[5] Wyrok TSUE z dnia 16 lipca 2020 r., Data Protection Commissioner przeciwko Facebook Ireland Limited i Maximillianowi Schremsowi, sprawa C-311/18, ECLI:UE:C:2020:559 (zwana dalej: „Schrems II").
[6] Zob. Schrems II, pkt 105.
[7] Zob. Schrems II, pkt 92.

8. Niezbędne gwarancje europejskie stanowią bowiem część oceny, którą należy przeprowadzić w celu ustalenia, czy państwo trzecie zapewnia stopień ochrony merytorycznie równoważny temu gwarantowanemu w UE, ale same w sobie nie mają na celu określenia wszystkich elementów niezbędnych do uznania, że dane państwo trzecie zapewnia taki stopień ochrony zgodnie z art. 45 RODO. Nie wskazują one również wszystkich elementów, które mogą być konieczne do rozważenia przy ocenie, czy system prawny państwa trzeciego uniemożliwia podmiotowi przekazującemu i odbierającemu dane zapewnienie odpowiednich zabezpieczeń zgodnie z art. 46 RODO.

9. W związku z tym elementy przedstawione w niniejszym dokumencie powinny być postrzegane jako niezbędne gwarancje, jakie należy znaleźć w państwie trzecim w trakcie oceny ingerencji w prawa do prywatności i ochrony danych, związanej ze środkami nadzoru państwa trzeciego, a nie jako wykaz elementów wykazujących, że system prawny państwa trzeciego jako całość zapewnia zasadniczo równoważny poziom ochrony.

10. Artykuł 6 ust. 3 Traktatu o Unii Europejskiej stanowi, że prawa podstawowe zapisane w EKPC są ogólnymi zasadami prawa UE. Jednakże, jak przypomina TSUE w swoim orzecznictwie, to ostatnie nie stanowi, dopóki Unia Europejska nie przystąpi do niego, instrumentu prawnego, który został formalnie włączony do prawa UE.[8] Stopień ochrony praw podstawowych wymagany na mocy art. 46 ust. 1 RODO należy zatem określić na podstawie przepisów tego rozporządzenia w świetle praw podstawowych zapisanych w Karcie. Mając na uwadze powyższe, zgodnie z art. 52 ust. 3 Karty, prawa w niej zawarte, odpowiadające prawom zagwarantowanym przez EKPC, mają mieć takie samo znaczenie i taki sam zakres jak prawa określone w tej konwencji, w związku z czym, jak przypomniał TSUE, należy uwzględnić orzecznictwo ETPC dotyczące praw, które są również przewidziane w Karcie praw podstawowych Unii Europejskiej, jako minimalny próg ochrony w celu interpretacji odpowiednich praw w Karcie[9]. Jednakże zgodnie z ostatnim zdaniem art. 52 ust. 3 Karty „[n]iniejsze postanowienie nie stanowi przeszkody, aby prawo Unii przyznawało szerszą ochronę".

11. W związku z tym istota niezbędnych gwarancji nadal będzie częściowo oparta na orzecznictwie ETPC, w zakresie, w jakim Karta zgodnie z wykładnią TSUE nie przewiduje wyższego stopnia ochrony, który nakazuje inne wymogi niż orzecznictwo ETPC.

12. Niniejszy dokument wyjaśnia kontekst i szczegóły czterech niezbędnych gwarancji europejskich.

2. INGERENCJE W PRAWA PODSTAWOWE

13. Podstawowe prawa do poszanowania życia prywatnego i rodzinnego, w tym komunikacji, oraz do ochrony danych osobowych są określone w art. 7 i 8 Karty i mają zastosowanie do wszystkich osób. Ponadto w art. 8 określono warunki zgodności z prawem przetwarzania danych osobowych oraz uznano prawo dostępu do danych i ich sprostowania, a także nałożono wymóg, aby przepisy te podlegały kontroli niezależnego organu.

[8] Zob. Schrems II, pkt 98.
[9] Zob. sprawy połączone C-511/18, C-512/18 i C-520/18, La Quadrature du Net i in. (zwane dalej La Quadrature du Net i in.), pkt 124.

14. „[O]peracja polegająca na przekazywaniu danych osobowych z państwa członkowskiego do państwa trzeciego stanowi jako taka przetwarzanie danych osobowych”[10]. W związku z tym art. 7 i art. 8 Karty mają zastosowanie do tej konkretnej operacji, a ochrona przez nie zapewniania obejmuje również przekazywane dane, dlatego też osobom, których dane osobowe są przekazywane do państwa trzeciego, należy zapewnić stopień ochrony zasadniczo odpowiadający stopniowi ochrony zapewnianemu w Unii Europejskiej.[11]

15. Zdaniem TSUE, gdy dochodzi do naruszenia podstawowego prawa do poszanowania życia prywatnego, zapisanego w art. 7 Karty, przez przetwarzanie danych osobowych osoby fizycznej naruszane jest również prawo do ochrony danych, ponieważ takie przetwarzanie wchodzi w zakres stosowania art. 8 Karty i w związku z tym musi koniecznie spełniać wymóg ochrony danych określony w tym artykule.[12]

16. Dlatego też, jeżeli chodzi o ewentualną ingerencję w prawa podstawowe wynikające z prawa UE, obowiązek nałożony na dostawców usług łączności elektronicznej (...) do zatrzymywania danych o ruchu w celu udostępnienia ich, w razie potrzeby, właściwym organom krajowym, budzi wątpliwości co do zgodności z art. 7 i 8 Karty[13]. To samo dotyczy innych rodzajów przetwarzania danych, takich jak przekazywanie danych osobom innym niż użytkownicy lub dostęp do tych danych w celu ich wykorzystania[14], co w związku z tym pociąga za sobą ingerencję w te prawa podstawowe. Ponadto zgodnie z utrwalonym orzecznictwem dostęp do danych przez organ publiczny stanowi dalszą ingerencję.[15]

17. W celu stwierdzenia ingerencji nie ma znaczenia, „czy informacje dotyczące życia prywatnego mają charakter wrażliwy i bez względu na to, czy z powodu tej ingerencji zainteresowane osoby doświadczyły ewentualnych niedogodności”[16]. Trybunał podkreślił również, że to, czy zatrzymane dane zostały następnie wykorzystane, jest bez znaczenia[17].

18. Niemniej jednak prawa ustanowione w art. 7, 8 i 11 Karty nie wydają się stanowić prerogatyw o charakterze absolutnym, lecz należy je rozważać z uwzględnieniem ich funkcji społecznej[18].

19. Karta zawiera test niezbędności (konieczności) i proporcjonalności w celu określenia ograniczeń praw, które chroni. Artykuł 52 ust. 1 Karty określa zakres możliwych ograniczeń w artykułach 7 i 8, stwierdzając, że „Wszelkie ograniczenia w korzystaniu z praw i wolności uznanych w niniejszej Karcie muszą być przewidziane ustawą i szanować istotę tych praw i wolności. Z zastrzeżeniem zasady proporcjonalności, ograniczenia mogą być wprowadzone wyłącznie wtedy, gdy są konieczne i rzeczywiście odpowiadają celom interesu ogólnego uznawanym przez Unię lub potrzebom ochrony praw i wolności innych osób”.

[10] TSUE, Schrems II, pkt 83.
[11] TSUE, Schrems II, pkt 96.
[12] TSUE, Schrems II, pkt 170-171.
[13] TSUE, sprawa C-623/17, Privacy International (zwana dalej: Privacy International), pkt 60.
[14] TSUE, Privacy International, pkt 61.
[15] ETPC, Leander, pkt 48; ETPC, Rotaru pkt 46; TSUE, Digital Rights Ireland, pkt 35.
[16] TSUE, Schrems II, pkt 171 wraz z przywołanym orzecznictwem.
[17] TSUE, Schrems II, pkt 171 wraz z przywołanym orzecznictwem.
[18] TSUE, Privacy International, pkt 63.

20. TSUE powtórzył, że uregulowanie UE, pociągające za sobą ingerencję w prawa podstawowe zagwarantowane przez art. 7 i 8 Karty, „musi zawierać jasne i precyzyjne przepisy regulujące zakres i sposób stosowania rozpatrywanego środka oraz ustanawiające minimalne wymogi służące temu, aby osoby, o których dane osobowe chodzi, miały wystarczające gwarancje pozwalające na skuteczną ochronę tych danych przed ryzykiem nadużyć”, zwłaszcza gdy dane osobowe są przetwarzane automatycznie oraz „kiedy występuje znaczne ryzyko nieuprawnionego dostępu do tych danych”.[19]

21. Zdaniem TSUE ochrona prawa do prywatności wymaga, aby wyjątki od prawa do ochrony danych i ograniczenia tego prawa „musiały być stosowane w zakresie, w jakim jest to absolutnie niezbędne”. Ponadto cel leżący w interesie ogólnym należy pogodzić z prawami podstawowymi, których dotyczy dany środek, „dokonując zbilansowanego wyważenia” między takim celem a rozpatrywanymi prawami.[20]

22. W związku z tym dostęp, zatrzymywanie i dalsze wykorzystywanie danych osobowych przez organy publiczne w ramach środków nadzoru nie może wykraczać poza to, co jest ściśle konieczne, oceniane w świetle Karty, w przeciwnym razie „nie może być uważane za uzasadnione w społeczeństwie demokratycznym”.[21]

23. Cztery niezbędne gwarancje europejskie, opracowane w następnym rozdziale, mają na celu doprecyzowanie, w jaki sposób oceniać poziom ingerencji w podstawowe prawa do prywatności i ochrony danych w kontekście środków nadzoru stosowanych przez organy publiczne w państwie trzecim przy przekazywaniu danych osobowych oraz jakie wymogi prawne muszą w związku z tym mieć zastosowanie, aby ocenić, czy takie ingerencje byłyby dopuszczalne na mocy Karty.

3. NIEZBĘDNE GWARANCJE EUROPEJSKIE

24. Po przeprowadzeniu analizy orzecznictwa EROD uważa, że mające zastosowanie wymogi prawne w celu uzasadnienia ograniczeń praw do ochrony danych i prywatności uznanych w Karcie można podsumować w czterech niezbędnych gwarancjach europejskich:

A. przetwarzanie powinno być oparte na jasnych, precyzyjnych i dostępnych zasadach;
B. należy wykazać niezbędność i proporcjonalność w odniesieniu do uzasadnionych zamierzonych celów;
C. powinien istnieć mechanizm niezależnej kontroli;
D. skuteczne środki ochrony prawnej muszą być dostępne dla osób fizycznych

25. Gwarancje te opierają się na niezbędnych prawach do prywatności i ochrony danych osobowych, które mają zastosowanie do wszystkich osób, niezależnie od obywatelstwa.

[19] TSUE, Privacy International, pkt 68 wraz z przywołanym orzecznictwem.
[20] TSUE, Privacy International, pkt 68 wraz z przywołanym orzecznictwem.
[21] TSUE, Privacy International, pkt 81.

Gwarancja A - Przetwarzanie powinno opierać się na jasnych, precyzyjnych i dostępnych zasadach

26. Zgodnie z art. 8 ust. 2 Karty dane osobowe powinny być między innymi przetwarzane „w określonych celach i za zgodą osoby zainteresowanej lub na innej uzasadnionej podstawie przewidzianej ustawą”,[22] jak przypomniał TSUE w orzeczeniu w sprawie Schrems II. Ponadto, zgodnie z art. 52 ust. 1 Karty, wszelkie ograniczenia w korzystaniu z praw i wolności uznanych w Karcie muszą w UE być przewidziane ustawą. W związku z tym uzasadniona ingerencja musi być zgodna z prawem.

27. Ta podstawa prawna powinna określać jasne i precyzyjne zasady regulujące zakres i stosowanie danego środka oraz nakładające minimalne zabezpieczenia[23]. Ponadto Trybunał przypomniał, że „to uregulowanie musi być prawnie wiążące w prawie krajowym”[24]. W tym względzie TSUE wyjaśnił, że ocena mającego zastosowanie prawa państwa trzeciego powinna koncentrować się na tym, czy osoby fizyczne mogą się na nie powoływać i polegać na nim przed sądem[25]. Trybunał stwierdza zatem, że prawa przyznane osobom, których dane dotyczą, powinny być egzekwowalne przed sądami; jeżeli osobom fizycznym nie zapewnia się praw egzekwowalnych wobec organów publicznych, przyznanego poziomu ochrony nie można uznać za merytorycznie równoważnego temu gwarantowanemu w Karcie, wbrew wymogom ustanowionym w art. 45 ust. 2 lit. a) RODO.[26]

28. Ponadto Trybunał podkreślił, że prawo właściwe musi wskazywać, w jakich okolicznościach i w jakich warunkach można przyjąć środek przewidujący przetwarzanie takich danych[27] (zob. poniżej w sekcji „Gwarancja B” związek między tymi wymogami a zasadami niezbędności i proporcjonalności).

29. TSUE wskazał również, że „wymóg, zgodnie z którym wszelkie ograniczenia korzystania z praw podstawowych muszą być przewidziane ustawą, oznacza, że podstawa prawna, która pozwala na ingerencję w te prawa, musi sama określać zakres ograniczenia wykonywania danego prawa”.[28]

30. Ponadto Europejski Trybunał Praw Człowieka „nie uważa, że nie ma żadnych podstaw do stosowania różnych zasad obejmujących z jednej strony dostępność i przejrzystość przepisów regulujących przechwytywanie konkretnej komunikacji konkretnych osób a z drugiej strony, bardziej ogólne programy inwigilacji”[29]. ETPC wyjaśnił również, że podstawa prawna powinna obejmować co najmniej definicję kategorii osób, które mogą podlegać inwigilacji, ograniczenie czasu trwania środka, procedurę, której należy przestrzegać przy badaniu, wykorzystywaniu i przechowywaniu uzyskanych danych, a także środki ostrożności, jakie należy podjąć przy przekazywaniu danych innym stronom.[30]

[22] Zob. Schrems II, pkt 173.
[23] Zob. Schrems II, pkt 175 i 180 oraz opinia 1/15 (umowa UE–Kanada o danych PNR) z dnia 26 lipca 2017 r., pkt 139 wraz z przywołanym orzecznictwem.
[24] Zob. Privacy International, pkt 68 – powinno być również jasne, że we francuskiej wersji wyroku Trybunał posługuje się terminem „réglementation”, które jest szersze niż tylko akty Parlamentu.
[25] Zob. Schrems II, pkt 181; gdzie TSUE odwołuje się do prezydenckiej dyrektywy politycznej nr 28.
[26] Zob. Schrems II, pkt 181.
[27] Zob. Privacy International, pkt 68 w odniesieniu do prawa państw członkowskich.
[28] Zob. Schrems II, pkt 175 wraz z przywołanym orzecznictwem oraz Privacy International, pkt 65.
[29] ETPC, Liberty, pkt 63.
[30] ETPC, Weber i Saravia, pkt 95.

31. Ingerencja musi być również przewidywalna w odniesieniu do jej skutków dla jednostki, aby zapewnić jej odpowiednią i skuteczną ochronę przed arbitralnymi ingerencjami i ryzykiem nadużyć. W związku z tym przetwarzanie danych musi opierać się na precyzyjnej, jasnej, ale również dostępnej (tzn. publicznej) podstawie prawnej[31]. ETPC, odnosząc się do tej kwestii, przypomniał w sprawie Zakharov, że „wzmianka o «przewidywalności» w kontekście przechwytywania komunikatów nie może być taka sama jak w wielu innych dziedzinach”. Stwierdził, że w kontekście tajnych środków nadzoru, takich jak przechwytywanie komunikatów, „przewidywalność nie może oznaczać, że dana osoba powinna być w stanie przewidzieć, kiedy organy prawdopodobnie przechwycą jej komunikaty, tak aby mogła odpowiednio dostosować swoje zachowanie”. Biorąc jednak pod uwagę, że w tego rodzaju sytuacjach ryzyko arbitralności jest oczywiste „niezbędne jest posiadanie jasnych, szczegółowych zasad przechwytywania rozmów telefonicznych, zwłaszcza że dostępna technologia jest coraz bardziej wyrafinowana. Prawo krajowe musi być wystarczająco jasne, aby dać obywatelom odpowiednią wskazówkę co do okoliczności i warunków, na jakich władze publiczne są uprawnione do stosowania takich środków”.[32]

Gwarancja B - Należy wykazać konieczność i proporcjonalność w odniesieniu do zgodnych z prawem zamierzonych celów

32. Zgodnie z pierwszym zdaniem art. 52 ust. 1 Karty wszelkie ograniczenia w korzystaniu z praw i wolności uznanych w Karcie muszą szanować istotę tych praw i wolności. Zgodnie z drugim zdaniem art. 52 ust. 1 Karty, w zastrzeżeniem zasady proporcjonalności, ograniczenia mogą być wprowadzone wyłącznie wtedy, gdy są konieczne i rzeczywiście odpowiadają celom interesu ogólnego uznawanym przez Unię lub potrzebom ochrony praw i wolności innych osób[33].

33. Jeśli chodzi o **zasadę proporcjonalności**, Trybunał orzekł, w odniesieniu do przepisów państw członkowskich, że kwestię, czy ograniczenie prawa do prywatności i ochrony danych może być uzasadnione, należy oceniać z jednej strony badając **wagę ingerencji** spowodowanej takim ograniczeniem[34] oraz z drugiej sprawdzając, czy **znaczenie celu interesu publicznym,** do którego zmierza to ograniczenie, jest proporcjonalne do wagi ingerencji[35].

34. W sprawie La Quadrature du net i in. można zauważyć, że TSUE orzekł w odniesieniu do prawa państwa członkowskiego, a nie prawa państwa trzeciego, że cel polegający na ochronie bezpieczeństwa narodowego może, ze względu na jego znaczenie, uzasadniać środki pociągające za sobą poważniejsze ingerencje w prawa podstawowe niż te, które mogłyby być uzasadnione innymi celami, takimi jak zwalczanie przestępczości. Trybunał uznał jednak, że tak jest, o ile istnieją wystarczająco solidne podstawy do uznania, że dane państwo stoi w obliczu poważnego zagrożenia dla bezpieczeństwa

[31] ETPC, Malone, pkt 65 i 66.
[32] ETPC, Zakharov, pkt 229.
[33] Schrems II, pkt 174.
[34] W tym kontekście Trybunał uznał np., że „ingerencja wynikająca z gromadzenia w czasie rzeczywistym danych umożliwiających lokalizację urządzeń końcowych wydaje się szczególnie poważna, ponieważ dane te zapewniają właściwym organom krajowym środki umożliwiające dokładne i trwałe śledzenie ruchu użytkowników telefonów komórkowych (...)”. (La Quadrature du Net i in., pkt 187 wraz z przywołanym orzecznictwem).
[35] La Quadrature du Net i in., pkt 131.

narodowego, które zostało wykazane jako rzeczywiste i aktualne lub możliwe do przewidzenia oraz z zastrzeżeniem spełnienia innych wymogów określonych w art. 52 ust. 1 Karty.[36]

35. W tym względzie zgodnie z utrwalonym orzecznictwem Trybunału odstępstwa od ochrony danych osobowych i jej ograniczenia powinny być stosowane jedynie w zakresie, w jakim jest to bezwzględnie konieczne[37]. W celu spełnienia tego wymogu, oprócz ustanowienia jasnych i precyzyjnych zasad dotyczących zakresu i stosowania danego środka, omawiane przepisy muszą ustanawiać minimalne gwarancje, tak aby osoby, których dane zostały przekazane, dysponowały wystarczającymi gwarancjami skutecznej ochrony ich danych osobowych przed ryzykiem nadużyć. „Powinno ono w szczególności wskazywać, w jakich okolicznościach i pod jakimi warunkami może zostać przyjęty środek przewidujący przetwarzanie takich danych, gwarantując w ten sposób, że ingerencja będzie ograniczona do tego, co ściśle konieczne. Konieczność zaopatrzenia w takie gwarancje jest istotna jeszcze bardziej wówczas, gdy dane osobowe są przetwarzane w sposób zautomatyzowany".[38]

36. W sprawie Schrems II TSUE podkreślił, że ustawodawstwo państwa trzeciego, które nie wskazuje żadnych ograniczeń przyznanych mu uprawnień do wdrażania programów nadzoru do celów wywiadu zagranicznego, nie może zapewnić stopnia ochrony merytorycznie równoważnego temu gwarantowanemu przez Kartę. Zgodnie z orzecznictwem podstawa prawna umożliwiająca ingerencję w prawa podstawowe musi bowiem, w celu spełnienia wymogów zasady proporcjonalności, sama określać zakres wykonywania danego prawa.[39]

37. Odnosząc się do **zasady niezbędności**, TSUE wyjaśnił, że uregulowanie „umożliwiające generalnie przechowywanie wszelkich danych osobowych wszystkich osób fizycznych, których dane zostały przekazane z Unii Europejskiej (...) bez jakiegokolwiek zróżnicowania, ograniczenia lub wyjątku w zależności od zamierzonego celu i bez przewidzenia obiektywnych kryteriów, które pozwoliłyby na ograniczenie dostępu władz publicznych do danych oraz na ich późniejsze wykorzystanie do określonych celów, ściśle ograniczonych, które mogą uzasadnić ingerencję, jaką stanowi zarówno dostęp, jak i wykorzystanie tych danych" nie jest zgodne z tą zasadą.[40] W szczególności należy uznać, że przepisy

[36] Pkt 136 i 137. Zob. również sprawę Privacy International, w której Trybunał uznał, że takie zagrożenia można odróżnić ze względu na swój charakter i szczególną wagę od ogólnego ryzyka wystąpienia napięć lub zakłóceń, nawet poważnych, mających wpływ na bezpieczeństwo publiczne. Pkt 75. Na przykład w wyroku La Quadrature du Net i in. Trybunał zauważył, że zautomatyzowana analiza danych o ruchu i lokalizacji obejmująca w sposób ogólny i niezróżnicowany dane osób korzystających z systemów łączności elektronicznej stanowi szczególnie poważną ingerencję, a zatem środek taki może spełniać wymóg proporcjonalności jedynie w sytuacjach, w których dane państwo członkowskie stoi w obliczu poważnego zagrożenia dla bezpieczeństwa narodowego, które zostało wykazane jako rzeczywiste i aktualne lub przewidywalne, oraz, oprócz innych warunków, pod warunkiem że okres zatrzymywania danych jest ograniczony do tego, co jest ściśle konieczne.

[37] Schrems II, pkt 176 wraz z przywołanym orzecznictwem.

[38] Schrems II, pkt 175.

[39] Schrems II, pkt 180.

[40] Schrems I, pkt 93 wraz z przywołanym orzecznictwem. Zob. jednak tym razem w odniesieniu do prawa państwa członkowskiego, a nie prawa państwa trzeciego, Privacy International, pkt 71, w tym cytowane orzecznictwo. W niniejszej sprawie Trybunał stwierdził, że przepisy państwa członkowskiego, które nakładają na dostawców usług łączności elektronicznej obowiązek ujawniania danych o ruchu i danych o lokalizacji agencjom bezpieczeństwa i wywiadu w drodze ogólnego i niezróżnicowanego przekazywania danych, wykraczają poza granice tego, co jest absolutnie niezbędne i nie można ich uznać za uzasadnione w społeczeństwie demokratycznym, zgodnie z wymogami dyrektywy o prywatności i łączności elektronicznej, czytanej w świetle Karty (ust. 81).

umożliwiające organom władzy publicznej ogólny dostęp do treści łączności elektronicznej naruszają istotę prawa podstawowego do poszanowania życia prywatnego, zagwarantowanego w art. 7 Karty.[41]

38. Tym razem jednak przy ocenie prawa państwa członkowskiego, a nie prawa państwa trzeciego, TSUE orzekł w sprawie La Quadrature du Net i in., że „ustawodawstwo nakładające obowiązek zatrzymywania danych osobowych musi zawsze spełniać obiektywne kryteria, które określają związek między zatrzymanymi danymi a zamierzonym celem"[42]. W tym samym kontekście w sprawie Privacy International Trybunał orzekł również, że prawodawca „musi opierać się na obiektywnych kryteriach w celu określenia okoliczności i warunków, na jakich właściwe organy krajowe mają uzyskać dostęp do przedmiotowych danych".[43]

Gwarancja C - Mechanizm niezależnego nadzoru

39. EROD przypomina, że ingerencja ma miejsce w momencie gromadzenia danych, ale również w momencie uzyskania dostępu do danych przez organ publiczny w celu ich dalszego przetwarzania. ETPC wielokrotnie stwierdzał, że wszelka ingerencja w prawo do prywatności i ochrony danych powinna podlegać skutecznemu, niezależnemu i bezstronnemu systemowi nadzoru, który musi być zapewniony przez sędziego lub inny niezależny organ[44] (np. organ administracyjny lub parlamentarny). Niezależny nadzór nad wdrażaniem środków nadzoru został również uwzględniony przez TSUE w wyroku w sprawie Schrems II.[45]

40. ETPC uściśla, że chociaż uprzednie (sądowe) zezwolenie na stosowanie środków nadzoru jest ważnym zabezpieczeniem przed arbitralnością, należy również wziąć pod uwagę rzeczywiste funkcjonowanie systemu przechwytywania, w tym mechanizmy kontroli i równowagi w zakresie wykonywania władzy, oraz istnienie lub brak faktycznego nadużycia[46]. W sprawie Schrems II TSUE uwzględnił również zakres funkcji nadzorczej mechanizmu nadzoru, który nie obejmował indywidualnych środków nadzoru.[47]

[41] Schrems I, pkt 94.

[42] La Quadrature du Net i in., pkt 133. W tym kontekście Trybunał potwierdził, że dyrektywa o prywatności i łączności elektronicznej, czytana w świetle Karty, sprzeciwia się środkom ustawodawczym przewidującym, jako środek zapobiegawczy, ogólne i masowe zatrzymywanie danych o ruchu i danych dotyczących lokalizacji. Trybunał orzekł natomiast, że w sytuacjach poważnego zagrożenia dla bezpieczeństwa narodowego, które zostało wykazane jako rzeczywiste i aktualne lub możliwe do przewidzenia, prawodawca może zezwolić, w celu zapewnienia bezpieczeństwa narodowego, na zastosowanie instrukcji zobowiązującej dostawców usług łączności elektronicznej do przechowywania, w sposób ogólny i niedyskryminujący, danych o ruchu i lokalizacji. Środek taki musi jednak spełniać szczególne warunki. W szczególności nakaz może być wydany jedynie na czas ograniczony do tego, co jest ściśle niezbędne, który może zostać przedłużony w przypadku utrzymywania się tego zagrożenia (pkt 168).

[43] Privacy International, pkt 78 wraz z przywołanym orzecznictwem W sprawie Privacy International, w odniesieniu do dostępu organu do danych osobowych przekazanych na mocy prawa państwa członkowskiego, Trybunał orzekł, że „ogólny dostęp do wszystkich zatrzymanych danych, niezależnie od jakiegokolwiek związku, nawet pośredniego, z realizowanym celem nie może być uważany za ograniczony do tego, co absolutnie niezbędne" (pkt 77 -78).

[44] ETPC, Klass, pkt 17 i 51.

[45] Schrems II, pkt 179 i 183

[46] ETPC, Big Brother Watch w postępowaniu apelacyjnym, pkt 319-320.

[47] Schrems II, pkt 179.

41. W odniesieniu do prawa państw członkowskich TSUE zidentyfikował szereg środków, które są zgodne z prawem UE tylko wtedy, gdy podlegają skutecznej kontroli przeprowadzanej przez sąd lub niezależny organ administracyjny, którego decyzja jest wiążąca. Celem tej kontroli jest sprawdzenie, czy istnieje sytuacja uzasadniająca dany środek oraz czy przestrzegane są warunki i gwarancje, które należy ustanowić[48]. W przypadku gromadzenia danych o ruchu i lokalizacji w czasie rzeczywistym przegląd powinien umożliwić sprawdzenie *ex ante*, między innymi, czy jest to dozwolone wyłącznie w granicach tego, co jest absolutnie niezbędne. W przypadku należycie uzasadnionej pilnej potrzeby środki mogą być zastosowane bez takiej uprzedniej kontroli; Trybunał nadal jednak wymaga, aby kolejna kontrola została przeprowadzona w krótkim czasie.[49]

42. Jeżeli chodzi o niezależność mechanizmów kontroli w odniesieniu do środków nadzoru, można by uwzględnić ustalenia TSUE dotyczące niezależności organu w kontekście środków ochrony prawnej (zob. poniżej w ramach gwarancji D). Dodatkowe elementy znaleźć można w orzecznictwie ETPC. Trybunał ten opowiedział się za tym, aby to sędzia był odpowiedzialny za prowadzenie nadzoru. Nie jest jednak wykluczone, że inny organ może być odpowiedzialny „o ile jest wystarczająco niezależny od władzy wykonawczej"[50] oraz „władz prowadzących nadzór, a także posiada wystarczające uprawnienia i kompetencje do sprawowania skutecznej i ciągłej kontroli".[51] ETPC dodał, że w ocenie niezależności należy wziąć pod uwagę „sposób powoływania i status prawny członków organu sprawującego nadzór".[52] Obejmuje to „osoby uprawnione do sprawowania urzędu sądowego, mianowane przez parlament lub przez premiera. Natomiast minister spraw wewnętrznych, który nie tylko jest osobą z nominacji politycznej, ale i członkiem władzy wykonawczej, bezpośrednio zaangażowanym we wdrażanie szczególnych środków nadzoru, został uznany za niewystarczająco niezależnego"[53]. ETPC „zauważa również, że istotne jest, aby organ nadzorczy miał dostęp do wszystkich istotnych dokumentów, w tym do materiałów niejawnych"[54]. Ponadto ETPC bierze pod uwagę, „czy działalność organu nadzorczego jest otwarta na publiczną kontrolę".[55]

Gwarancja D - Skuteczne środki ochrony prawnej muszą być dostępne dla osób fizycznych

43. Ostatnia niezbędna gwarancja europejska związana jest z prawami osób fizycznych do dochodzenia roszczeń. Osoba musi dysponować skutecznym środkiem prawnym w celu wyegzekwowania swoich praw, jeżeli uzna, że nie są one przestrzegane lub nie były przestrzegane. TSUE wyjaśnił w wyroku w Schrems I, że „uregulowanie nieprzewidujące dla jednostek żadnej drogi prawnej w celu uzyskania dostępu do dotyczących ich danych osobowych lub sprostowania czy usunięcia takich danych nie zapewnia poszanowania zasadniczej istoty prawa podstawowego do skutecznej ochrony prawnej, wynikającego z art. 47 Karty. Artykuł 47 akapit pierwszy Karty stanowi bowiem, że każdy, kogo prawa i

[48] TSUE, La Quadrature du Net i in., pkt 168 i 189.
[49] TSUE, La Quadrature du Net i in., pkt 189.
[50] ETPC, Zakharov, pkt 258, Iordachi i in. przeciwko Mołdawii, pkt 40 i 51, a także Dumitru Popescu przeciwko Rumunii, pkt70-73.
[51] ETPC, Klass, pkt 56 i Big Brother Watch w postępowaniu apelacyjnym, pkt 318.
[52] ETPC, Zakharov, pkt 278.
[53] ETPC, Zakharov, pkt 278.
[54] ETPC, Zakharov, pkt 281.
[55] ETPC, Zakharov, pkt 283.

wolności zagwarantowane przez prawo Unii zostały naruszone, ma prawo do skutecznego środka prawnego przed sądem, zgodnie z warunkami przewidzianymi w tym artykule".[56]

44. Oceniając uregulowanie państwa członkowskiego, zezwalające na gromadzenie w czasie rzeczywistym danych o ruchu i danych o lokalizacji, Trybunał uznał, że powiadomienie jest konieczne, „aby umożliwić osobom, których dotyczy dany środek, skorzystanie z praw przysługujących im na mocy art. 7 i 8 Karty, tj. zażądanie dostępu do ich danych osobowych, które były przedmiotem tych środków, a także w stosownych przypadkach ich sprostowania lub usunięcia, oraz prawa do skutecznego środka prawnego przed sądem, zgodnie z art. 47 akapit pierwszy Karty".[57] Trybunał uznał jednak również, że powiadomienie osób, których dane zostały zebrane lub poddane analizie, musi nastąpić tylko w takim zakresie i w takim czasie, w jakim powiadomienie nie zagraża już zadaniom, za które organy te są odpowiedzialne[58].

45. Również dla ETPC kwestia skutecznego środka ochrony prawnej jest nierozłącznie związana z powiadomieniem danej osoby o środku nadzoru po tym, jak nadzór został zakończony. W szczególności Trybunał stwierdził, że „osoba zainteresowana ma co do zasady niewielkie możliwości odwołania się do sądu, chyba że osoba ta zostanie powiadomiona o środkach podjętych bez jej wiedzy i tym samym może zakwestionować ich zgodność z prawem wstecznie lub ewentualnie, osoba, która podejrzewa, że jej komunikaty są lub zostały przechwycone, może zwrócić się do sądów, tak że jurysdykcja sądów nie zależy od powiadomienia osoby podlegającej przechwytywaniu o przechwyceniu jej wiadomości"[59]. ETPC uznał zatem, że w niektórych przypadkach powiadomienie może nie mieć miejsca, należy jednak zapewnić skuteczny środek ochrony prawnej. W niniejszej sprawie Trybunał wyjaśnił, na przykład w sprawie Kennedy, że sąd oferuje wystarczające możliwości dochodzenia roszczeń, jeżeli spełnia szereg kryteriów, tj. niezależny i bezstronny organ, który przyjął własny regulamin postępowania, składający się z członków, którzy muszą sprawować lub sprawowali wysokie stanowiska sądowe lub być doświadczonymi prawnikami, oraz że nie ma żadnych obciążeń dowodowych, które można by pokonać, aby złożyć do niego wniosek[60]. Rozpatrując skargi osób fizycznych, sąd powinien mieć dostęp do wszystkich istotnych informacji,[61] w tym materiałów niejawnych. Ponadto powinien on mieć uprawnienia do usunięcia niezgodności.[62]

46. Artykuł 47 Karty odwołuje się do trybunału, nawet jeśli w wersjach językowych innych niż angielska preferowane jest słowo „sąd",[63] natomiast EKPC nakłada na państwa członkowskie jedynie obowiązek zapewnienia, że „każdy, kogo prawa i wolności zostały naruszone, ma prawo do skutecznego środka

[56] TSUE, Schrems I, pkt 95.
[57] Zob. La Quadrature du Net i in., pkt 190 oraz opinia TSUE 1/15, pkt 220.
[58] Zob. La Quadrature du Net i in., pkt 191.
[59] ETPC, Zakharov, pkt 234.
[60] ETPC, Kennedy, pkt 190.
[61] EROD dostrzega, że zdaniem Komisarza Praw Człowieka Rady Europy tzw. zasada „stron trzecich" (zgodnie z którą agencje wywiadowcze jednego kraju, dostarczające dane agencjom wywiadowczym innego, mogą nakładać na agencje otrzymujące obowiązek nieujawniania przekazanych danych żadnej stronie trzeciej) nie powinna mieć zastosowania do organów nadzorujących, aby nie podważać możliwości skutecznego środka ochrony prawnej (dokument tematyczny w sprawie demokratycznej i skutecznej kontroli nad krajowymi służbami bezpieczeństwa).
[62] ETPC, Kennedy, pkt 167.
[63] Słowo „trybunał" tłumaczone jest na przykład jako „Gericht" w języku niemieckim i „gerecht" w języku holenderskim.

odwoławczego do właściwego organu państwowego",[64] który niekoniecznie musi być organem sądowym.[65]

47. W kontekście wyroku w sprawie Schrems II TSUE, oceniając adekwatność stopnia ochrony państwa trzeciego, powtórzył, że „jednostkom powinna przysługiwać możliwość skorzystania przed niezawisłym i bezstronnym sądem ze środków prawnych w celu uzyskania dostępu do dotyczących ich danych osobowych lub spowodowania korekty lub usunięcia takich danych".[66] W tym samym kontekście TSUE uważa, że skuteczna ochrona sądowa przed takimi ingerencjami może być zapewniona nie tylko przez sąd, ale również przez organ,[67] który zapewnia gwarancje merytorycznie równoważne tym wymaganym na mocy art. 47 Karty. W orzeczeniu w sprawie Schrems II TSUE podkreślił, że należy zapewnić niezależność sądu lub organu, zwłaszcza władzy wykonawczej, ze wszystkimi niezbędnymi gwarancjami, w tym w odniesieniu do warunków odwołania[68] oraz że uprawnienia, które powinny zostać przyznane sądowi, muszą być zgodne z wymogami art. 47 Karty. W tym względzie organowi[69] przyznaje się uprawnienia do przyjmowania decyzji wiążących służby wywiadowcze, zgodnie z gwarancjami prawnymi, na których mogłyby się opierać osoby, których dane dotyczą[70].

4. UWAGI KOŃCOWE

48. Cztery niezbędne gwarancje europejskie należy postrzegać jako podstawowe elementy oceny poziomu ingerencji w podstawowe prawa do prywatności i ochrony danych. Nie powinny one być oceniane niezależnie, ponieważ są ściśle ze sobą powiązane, lecz w ujęciu ogólnym, dokonując przeglądu odpowiednich przepisów w odniesieniu do środków nadzoru, minimalnego poziomu gwarancji ochrony praw osób, których dane dotyczą, oraz środków ochrony prawnej przewidzianych w prawie krajowym państwa trzeciego.

49. Gwarancje te wymagają pewnego stopnia interpretacji, zwłaszcza że przepisy państw trzecich nie muszą być identyczne z ramami prawnymi UE.

50. Jak stwierdził ETPC w sprawie Kennedy, „ocena zależy od wszystkich okoliczności sprawy, takich jak charakter, zakres i czas trwania ewentualnych środków, podstawy wymagane do wydania nakazu, organy właściwe do ich zatwierdzenia, wdrożenia i kontroli oraz rodzaj środka ochrony prawnej przewidzianego w prawie krajowym".[71]

51. W związku z tym ocena środków nadzoru w państwach trzecich w stosunku do niezbędnych gwarancji europejskich (NGE) może prowadzić do dwóch wniosków:

[64] Artykuł 13 EKPC.
[65] ETPC, Klass, pkt 67.
[66] Zob. Schrems II, pkt 194.
[67] Zob. Schrems II, pkt 197, w którym Trybunał wyraźnie używa tego słowa.
[68] Zob. Schrems II, pkt 195.
[69] Zob. Schrems II, pkt 197, w którym Trybunał wyraźnie używa tego słowa.
[70] Zob. Schrems II, pkt 196.
[71] ETPC, Kennedy, pkt 153.

- Przedmiotowe uregulowania w państwach trzecich nie są zgodne z NGE: w takim przypadku ustawodawstwo państwa trzeciego nie zapewniałoby poziomu ochrony zasadniczo równoważnego z poziomem gwarantowanym w UE.

- Przedmiotowe uregulowania w państwach trzecich spełniają wymogi NGE.

52. Oceniając, czy stopień ochrony jest odpowiedni, zgodnie z art. 45 RODO Komisja będzie musiała ocenić, czy NGE są spełnione w ramach elementów, które należy uznać za gwarantujące, że prawodawstwo państwa trzeciego jako całość zapewnia stopień ochrony merytorycznie równoważny temu gwarantowanemu w UE.

53. Jeżeli podmioty przekazujące dane wraz z podmiotami odbierającymi dane opierają się na odpowiednich zabezpieczeniach na mocy art. 46 RODO, biorąc pod uwagę wymogi ustawodawstwa państwa trzeciego, mające szczególne zastosowanie do przekazywanych danych, musiałyby one zapewnić skuteczne osiągnięcie merytorycznie równoważnego stopnia ochrony. W szczególności, w przypadku gdy prawo państwa trzeciego nie spełnia wymogów NGE, oznaczałoby to zapewnienie, aby przedmiotowe prawo nie naruszało gwarancji i zabezpieczeń towarzyszących przekazaniu, tak aby stopień ochrony merytorycznie równoważny temu gwarantowanemu w UE był nadal zapewniany.

54. EROD wydała dalsze wytyczne i zalecenia, które należy uwzględnić przy przeprowadzaniu oceny, w zależności od narzędzia przekazywania danych, które należy zastosować, oraz od konieczności zapewnienia odpowiednich zabezpieczeń, w tym, w stosownych przypadkach, środków uzupełniających.[72]

55. Ponadto należy zauważyć, że niezbędne gwarancje europejskie opierają się na wymogach prawa. EROD podkreśla, że niezbędne gwarancje europejskie opierają się na prawach podstawowych, które mają zastosowanie do wszystkich osób, niezależnie od ich obywatelstwa.

56. EROD powtarza, że niezbędne gwarancje europejskie są standardem odniesienia przy ocenie ingerencji związanej ze środkami nadzoru państw trzecich w kontekście międzynarodowego przekazywania danych. Standardy te wynikają z prawa UE oraz z orzecznictwa TSUE i ETPC, które są wiążące dla państw członkowskich.

[72] Dokument „Odpowiedni stopień ochrony przekazywanych danych osobowych", WP 254 rev.01, Ostatnio zmieniony i przyjęty dnia 6 lutego 2018 r.; Zalecenia EROD nr 1/2020 w sprawie środków uzupełniających narzędzia przekazywania danych w celu zapewnienia zgodności z unijnym stopniem ochrony danych osobowych, 10 listopada 2020 r.



Translations proofread by EDPB Members.
This language version has not yet been proofread.

Zalecenia 01/2020 dotyczące środków uzupełniających narzędzia przekazywania w celu zapewnienia zgodności z unijnym stopniem ochrony danych osobowych

Przyjęte w dniu 10 listopada 2020 r.

Streszczenie

Przyjęcie ogólnego rozporządzenia UE o ochronie danych (RODO) miało służyć dwóm celom: ułatwieniu swobodnego przepływu danych osobowych na terytorium Unii Europejskiej, przy jednoczesnej ochronie podstawowych praw i wolności osób fizycznych, w szczególności prawa do ochrony danych osobowych.

W niedawno wydanym wyroku w sprawie C-311/18 (Schrems II) Trybunał Sprawiedliwości Unii Europejskiej (TSUE) przypomniał, że ochrona przyznana danym osobowym w Europejskim Obszarze Gospodarczym (EOG) musi towarzyszyć tym danym w każdym miejscu, do którego są przekazywane. Przekazanie danych osobowych do państwa trzeciego nie może prowadzić do rozluźnienia lub osłabienia ochrony zagwarantowanej w EOG. Trybunał wyjaśnił również, iż nie jest wymagane, aby państwa trzecie zapewniały stopień ochrony identyczny jak ten zagwarantowany w EOG, lecz jedynie merytorycznie równoważny. Trybunał potwierdził także ważność standardowych klauzul umownych jako narzędzia przekazywania, dzięki któremu można zapewnić na poziomie umownym merytorycznie równoważny stopień ochrony danych przekazywanych do państw trzecich.

Standardowe klauzule umowne i inne narzędzia przekazywania, o których mowa w art. 46 RODO, nie funkcjonują w próżni. Trybunał stwierdził, że administratorzy lub podmioty przetwarzające pełniący rolę podmiotów przekazujących dane są zobowiązani do sprawdzenia w każdym konkretnym przypadku i – gdy ma to zastosowanie – we współpracy z podmiotem odbierającym te dane w państwie trzecim, czy prawo lub praktyki państwa trzeciego mają negatywny wpływ na skuteczność odpowiednich zabezpieczeń zawartych w narzędziach przekazywania z art. 46 RODO. W takich przypadkach Trybunał wciąż pozostawia podmiotom przykazującym dane otwartą możliwość wdrożenia środków uzupełniających, które wypełniłyby luki w ochronie i podniosłyby ją do stopnia wymaganego przez prawo UE. Trybunał nie sprecyzował, jakie mogą to być środki. Wskazał jednak, że podmioty przekazujące dane będą musiał określać je w każdym konkretnym przypadku. Jest to zgodne z zasadą rozliczalności, o której mowa w art. 5 ust. 2 RODO, stanowiącą, że administrator jest odpowiedzialny za przestrzeganie zasad RODO dotyczących przetwarzania danych osobowych i musi być w stanie wykazać ich przestrzeganie.

Żeby wesprzeć podmioty przekazujące dane (niezależnie czy będą nimi administratorzy, podmioty przetwarzające, podmioty prywatne czy urzędy publiczne, które przetwarzają dane osobowe w zakresie zastosowania RODO) w skomplikowanym zadaniu polegającym na przeprowadzeniu oceny państw trzecich i w razie potrzeby określeniu odpowiednich środków uzupełniających, Europejska Rada Ochrony Danych (EROD) przyjęła niniejsze zalecenia. Przedstawiają one podmiotom przekazującym dane schemat działań, jakie należy podjąć, potencjalne źródła informacji, a także pewne przykłady środków uzupełniających, jakie można wprowadzić.

Pierwszym krokiem, jaki zdaniem EROD podmioty przekazujące dane powinny podjąć, jest **rozpoznanie przeprowadzanych operacji przekazywania**. Zidentyfikowanie wszystkich operacji przekazywania danych osobowych do państw trzecich może być bardzo trudnym zadaniem. Uświadomienie sobie, gdzie dane osobowe trafiają, jest niemniej jednak konieczne, żeby zapewnić merytorycznie równoważny stopień ochrony wszędzie tam, gdzie dane są przetwarzane. Należy także sprawdzić, czy dane, jakie zostaną przekazane, są adekwatne, stosowne i ograniczone do tego, co niezbędne do celów, dla których są one przekazywane i przetwarzane w państwie trzecim.

Drugi krok polega na **sprawdzeniu, czy wykorzystywane narzędzie przekazywania**, jest wymienione w rozdziale V RODO. Jeśli Komisja Europejska w drodze decyzji stwierdzającej odpowiedni stopień ochrony wydanej na podstawie art. 45 RODO lub poprzednio obowiązującej dyrektywy 95/46

stwierdziła już, że dane państwo, region lub sektor, do którego dane są przesyłane, oferuje odpowiedni stopień ochrony, to do momentu, aż decyzja taka przestanie obowiązywać, nie będzie trzeba podejmować żadnych dalszych działań poza monitorowaniem, czy taka decyzja stwierdzająca odpowiedni stopień ochrony pozostaje ważna. W przypadku braku decyzji stwierdzającej odpowiedni stopień ochrony konieczne będzie skorzystanie z jednego z narzędzi przekazywania, wymienionych w art. 46 RODO, jeśli operacje przekazywania są regularne i powtarzalne. Jedynie w przypadku sporadycznych i niepowtarzających się operacji przetwarzania możliwe będzie skorzystanie z jednego z wyjątków przewidzianych w art. 49 RODO, jeśli spełniono określone tam warunki.

Trzecim krokiem jest **ocena**, czy w **prawie lub praktyce państwa trzeciego** funkcjonuje cokolwiek, co w kontekście danej operacji przekazywania mogłoby negatywnie wpłynąć na skuteczność odpowiednich zabezpieczeń wykorzystywanych narzędzi przekazywania. Ocena powinna skupiać się przede wszystkim na przepisach państwa trzeciego, które znajdują zastosowanie do danej operacji przetwarzania i do wykorzystywanego narzędzia przetwarzania z art. 46 RODO, a które może doprowadzić do zmniejszenia stopnia jego ochrony. Przy analizie elementów, które trzeba uwzględnić w ocenie przepisów państwa trzeciego dotyczących dostępu organów publicznych do danych do celów nadzoru, należy odwołać się do zaleceń EROD w sprawie niezbędnych gwarancji europejskich. W szczególności należy dokładnie rozważyć, czy przepisy dotyczące dostępu organów publicznych do danych są niejednoznaczne lub nie są publicznie dostępne. Jeśli nie ma przepisów określających przypadki, gdy organy publiczne mogą uzyskać dostęp do danych osobowych, i niezależnie od tego operacja przekazywania ma się odbyć, należy przyjrzeć się innym istotnym i obiektywnym czynnikom, a nie polegać na czynnikach subiektywnych, takich jak prawdopodobieństwo, że organy publiczne uzyskają dostęp do danych w sposób niezgodny z normami UE. Ocenę tę należy przeprowadzić z należytą starannością i dokładnie ją udokumentować, jako że podmiot będzie rozliczany z decyzji, jaką może podjąć na tej podstawie.

Czwartym krokiem jest **określenie i przyjęcie środków uzupełniających**, jakie są konieczne, żeby stopień ochrony przekazywanych danych był merytorycznie równoważny temu gwarantowanemu na podstawie norm UE. Krok ten jest niezbędny tylko wtedy, gdy przeprowadzona ocena wykaże, iż przepisy państwa trzeciego mają w kontekście danej operacji przekazywania negatywny wpływ na skuteczność wykorzystywanego lub planowanego narzędzia przekazywania z art. 46 RODO. Zalecenia te zawierają (w załączniku nr 2) również niewyczerpujący wykaz przykładowych środków uzupełniających oraz niektórych warunków, które byłyby niezbędne do zapewnienia skuteczności. Podobnie jak w przypadku odpowiednich zabezpieczeń zawartych w narzędziach przekazywania wymienionych w art. 46 niektóre środki uzupełniające mogą być skuteczne w jednych państwach, ale niekoniecznie w innych. Będą Państwo odpowiedzialni za ocenę ich skuteczności w kontekście danej operacji przetwarzania, w świetle przepisów obowiązujących w państwie trzecim i wykorzystywanego narzędzia przekazywania, i rozliczani z podjętej decyzji. Może to także pociągnąć za sobą konieczność połączenia różnych środków uzupełniających. Ostatecznie może okazać się, że żaden środek uzupełniający nie zapewni merytorycznie równoważnego stopnia ochrony na potrzeby danej operacji przekazywania. W takim przypadku, gdy żaden środek uzupełniający nie będzie odpowiedni, należy odstąpić od przekazania danych, zawiesić lub zakończyć je, żeby uniknąć naruszenia stopnia ochrony danych osobowych. Powinni Państwo przeprowadzić tę ocenę z należytą starannością i udokumentować ją.

Piątym krokiem jest **podjęcie** wszelkich **formalnych kroków proceduralnych**, jakich wymagać może przyjęcie środka uzupełniającego w zależności od wykorzystywanego narzędzia przekazywania z art. 46 RODO. Niniejsze zalecenia wskazują, jakie są to formalności. W niektórych przypadkach koniecznie może być także skonsultowanie się z właściwym organem nadzorczym.

Szóstym i ostatnim krokiem będzie dokonanie ponownej oceny, w odpowiednich odstępach czasu, stopnia ochrony danych przekazywanych do państw trzecich i monitorowanie, czy wystąpiły lub wystąpią jakiekolwiek zmiany w tym zakresie. Zasada rozliczalności wymaga zachowania stałej czujności w odniesieniu do stopnia ochrony danych osobowych.

Organy nadzorcze będą nadal wykonywać swoje uprawnienia w zakresie monitorowania stosowania RODO i egzekwowania go. Będą one zwracać należytą uwagę na działania podejmowane przez podmioty przekazujące w celu zapewnienia, że przekazywane dane są objęte merytorycznie równoważnym stopniem ochrony. Jak przypomina Trybunał, organy nadzorcze są zobowiązane do zawieszenia lub zakazania przekazywania danych w przypadku, gdy po przeprowadzeniu dochodzenia lub na podstawie skargi stwierdzą, że nie można zapewnić merytorycznie równoważnego stopnia ochrony.

Organy nadzorcze będą nadal opracowywać wytyczne dla podmiotów przekazujących i koordynować swoje działania w ramach EROD w celu zapewnienia spójności w stosowaniu unijnych przepisów o ochronie danych.

Spis treści

1 Rozliczalność przy przekazywaniu danych 8
2 Plan działania: stosowanie zasady rozliczalności do przekazywania danych w praktyce 9
2.1 Krok 1: Rozpoznanie przeprowadzanych operacji przekazywania 9
2.2 Krok 2: Określenie wykorzystywanych narzędzi przekazywania 11
2.3 Krok 3: Ocena, czy wykorzystywane narzędzie przekazywania z art. 46 RODO jest skuteczne w świetle wszystkich okoliczności przekazywania 13
2.4 Krok 4: Przyjęcie środków uzupełniających 17
2.5 Krok 5: Podjęcie kroków proceduralnych w przypadku, gdy zidentyfikowano skuteczne środki uzupełniające 19
2.6 Krok 6: Ponowna ocena w odpowiednich odstępach czasu 21
3 Wnioski 22
ZAŁĄCZNIK 1: DEFINICJE 23
ZAŁĄCZNIK 2: PRZYKŁADY ŚRODKÓW UZUPEŁNIAJĄCYCH 24
Środki techniczne 24
Dodatkowe środki umowne 31
Środki organizacyjne 39
ZAŁĄCZNIK 3: MOŻLIWE ŹRÓDŁA INFORMACJI NA POTRZEBY OCENY PAŃSTWA TRZECIEGO 43

Europejska Rada Ochrony Danych

uwzględniając art. 70 ust. 1 lit. e) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (zwanego dalej „RODO"),

uwzględniając Porozumienie o Europejskim Obszarze Gospodarczym (EOG), a w szczególności jego załącznik XI i protokół 37, w brzmieniu zmienionym decyzją Wspólnego Komitetu EOG nr 154/2018 z dnia 6 lipca 2018 r.[1],

uwzględniając art. 12 i 22 swojego regulaminu wewnętrznego,

mając również na uwadze, co następuje:

(1) Trybunał Sprawiedliwości Unii Europejskiej (TSUE) w swoim wyroku z dnia 16 lipca 2020 r. w sprawie C-311/18 Data Protection Commissioner przeciwko Facebook Ireland LTD i Maximillianowi Schremsowi stwierdził, że art. 46 ust. 1 i art. 46 ust. 2 lit. c) RODO należy interpretować w ten sposób, że wymagane przez te przepisy odpowiednie zabezpieczenia, egzekwowalne prawa oraz skuteczne środki ochrony prawnej powinny zapewniać, by prawa osób, których dane osobowe są przekazywane do państwa trzeciego na podstawie klauzul ochrony danych, były chronione w stopniu merytorycznie równoważnym temu gwarantowanemu w Unii przez to rozporządzenie, interpretowane w świetle Karty praw podstawowych Unii Europejskiej[2].

(2) Jak Trybunał podkreślił, stopień ochrony osób fizycznych merytorycznie równoważny temu gwarantowanemu w Unii Europejskiej przez RODO interpretowane w świetle Karty powinien być zapewniony niezależnie od przepisu rozdziału V dotyczącego podstawy, na jakiej dokonywane jest przekazywanie danych osobowych do państwa trzeciego. Przepisy rozdziału V RODO mają na celu zapewnienie ciągłości stopnia tej ochrony w sytuacji, gdy dane te są przekazywane do państwa trzeciego[3].

(3) Motyw 108 i art. 46 ust. 1 RODO stanowią, że w razie braku unijnej decyzji stwierdzającej odpowiedni stopień ochrony administrator lub podmiot przetwarzający powinni zastosować środki rekompensujące brak ochrony danych w państwie trzecim, zapewniając osobie, której dane dotyczą, odpowiednie zabezpieczenia. Administrator lub podmiot przetwarzający mogą zapewnić odpowiednie zabezpieczenia bez konieczności uzyskania specjalnego zezwolenia ze strony organu nadzorczego poprzez zastosowanie jednego z narzędzi przekazywania wymienionych w art. 46 ust. 2 RODO, np. standardowych klauzul ochrony danych.

[1] Odniesienia do „państw członkowskich" w niniejszym dokumencie należy rozumieć jako odniesienia do „państw członkowskich EOG".
[2] Wyrok TSUE z dnia 16 lipca 2020 r. w sprawie C-311/18 Data Protection Commissioner przeciwko Facebook Ireland LTD i Maximillianowi Schremsowi (dalej: C-311/18 (Schrems II)), drugie ustalenie.
[3] C-311/18 (Schrems II), pkt 92 i 93.

(4) Trybunał wyjaśnił, że standardowe klauzule ochrony danych przyjęte przez Komisję mają na celu wyłącznie ustanowienie dla mających siedzibę w Unii administratorów danych lub podmiotów przetwarzających zabezpieczeń umownych znajdujących jednolite zastosowanie we wszystkich państwach trzecich. Ze względu na ich umowny charakter standardowe klauzule ochrony danych nie mogą wiązać organów władzy publicznej państw trzecich, ponieważ nie są one stronami zawartej umowy. W związku z powyższym może okazać się konieczne uzupełnienie tych zabezpieczeń zawartych w standardowych klauzulach ochrony danych poprzez podjęcie przez podmioty przekazujące dane środków uzupełniających mających na celu zapewnienie przestrzegania stopnia ochrony wymaganego na podstawie przepisów UE w państwie trzecim. Trybunał przywołuje motyw 109 RODO, który wspomina o takiej możliwości i zachęca administratorów i podmioty przetwarzające do korzystania z niej[4].

(5) Trybunał wskazał, że to przede wszystkim do podmiotu przekazującego dane należy sprawdzenie w każdym konkretnym przypadku i – gdy ma to zastosowanie – we współpracy z podmiotem odbierającym te dane, czy prawo państwa trzeciego przeznaczenia zapewnia merytorycznie równoważny, w świetle prawa Unii, stopień ochrony danych osobowych przekazywanych na podstawie standardowych klauzul ochrony danych, udzielając w razie potrzeby zabezpieczeń dodatkowych w stosunku do tych zapewnianych w tych klauzulach[5].
(6) W przypadku braku możliwości podjęcia przez mających siedzibę w Unii Europejskiej administratora danych lub podmiot przetwarzający środków uzupełniających odpowiednich dla zagwarantowania merytorycznie równoważnego stopnia ochrony w świetle prawa UE, podmioty te lub, pomocniczo, właściwy organ nadzorczy, są zobowiązane do zawieszenia lub zakończenia przekazywania danych osobowych do danego państwa trzeciego[6].
(7) Ani RODO, ani Trybunał nie podają definicji ani nie precyzują pojęć „zabezpieczeń dodatkowych", „dodatkowych środków" czy „środków uzupełniających" w stosunku do zabezpieczeń narzędzi przekazywania wymienionych w art. 46 ust. 2 RODO, które administratorzy i podmioty przetwarzające mogą przyjąć w celu zapewnienia przestrzegania wymaganego przez prawo UE stopnia ochrony w danym państwie trzecim.
(8) EROD z własnej inicjatywy podjęła decyzję o przeanalizowaniu tej kwestii i przedstawieniu zaleceń dla administratorów i podmiotów przetwarzających działających jako podmiot przekazujące w zakresie procedury, którą można zastosować w celu określenia i przyjęcia środków uzupełniających. Niniejsze zalecenia mają na celu dostarczenie podmiotom przekazującym metodologii, dzięki której możliwe będzie ustalenie, czy w odniesieniu do operacji przekazywania należy podjąć jakiekolwiek dodatkowe środki, a jeśli tak – jakie. Podstawowym obowiązkiem podmiotów przekazujących jest zapewnienie, że przekazywane dane są objęte w państwie trzecim merytorycznie równoważnym stopniem ochrony do tego gwarantowanego w UE. Za pomocą tych zaleceń EROD zgodnie ze swoją właściwością zachęca do konsekwentnego stosowania zarówno RODO, jak i orzeczenia Trybunału[7].

PRZYJMUJE NINIEJSZE ZALECENIA:

[4] C-311/18 (Schrems II), pkt 132 i 133.
[5] C-311/18 (Schrems II), pkt 134.
[6] C-311/18 (Schrems II), pkt 135.
[7] Art. 70 ust. 1 lit. e) RODO.

1 ROZLICZALNOŚĆ PRZY PRZEKAZYWANIU DANYCH

1. Prawo pierwotne UE uznaje prawo do ochrony danych za prawo podstawowe[8]. W związku z tym prawu do ochrony danych przyznaje się wysoki stopień ochrony, zaś wszelkie ograniczenia tego prawa można wprowadzać tylko wtedy, gdy są one przewidziane ustawą, szanują jego istotę, są proporcjonalne, niezbędne i rzeczywiście odpowiadają celom interesu ogólnego uznawanym przez Unię lub potrzebom ochrony praw i wolności innych osób[9]. Prawo do ochrony danych osobowych nie jest jednak prerogatywą o charakterze absolutnym, lecz powinno być rozpatrywane w kontekście jego funkcji społecznej i wyważone względem innych praw podstawowych w myśl zasady proporcjonalności[10].

2. Stopień ochrony merytorycznie równoważny temu gwarantowanemu w UE musi być zagwarantowany w odniesieniu do danych przekazywanych do państwa trzeciego spoza EOG, żeby zapewnić, iż nie naruszono stopnia ochrony gwarantowanego na podstawie RODO.

3. Prawo do ochrony danych ma czynny charakter. Wymaga ono od podmiotów przekazujących i podmiotów odbierających (zarówno administratorów, jak i podmiotów przetwarzających) czegoś więcej niż tylko uznania, że takie prawo istnieje, lub pasywnej zgodności z nim[11]. Administratorzy i podmioty przetwarzające są w obowiązku dążyć do przestrzegania prawa do ochrony danych w czynny i ciągły sposób poprzez wprowadzanie środków prawnych, technicznych i organizacyjnych, które zapewniają jego skuteczność. Administratorzy i podmioty przetwarzające muszą także być w stanie udowodnić osobom, których dane dotyczą, ogółowi społeczeństwa i organom nadzorczym odpowiedzialnym za ochronę danych, że takie działania są faktycznie podejmowane. Jest to tak zwana zasada rozliczalności[12].

4. Zasada rozliczalności, która jest konieczna do zapewnienia skutecznego stosowania stopnia ochrony przewidzianego w RODO, dotyczy również przekazywania danych do państw trzecich[13], jako że operacje tego rodzaju stanowią same w sobie formę przetwarzania danych[14]. Jak Trybunał podkreślił w wydanym wyroku, stopień ochrony merytorycznie równoważny temu zagwarantowanemu w Unii Europejskiej przez RODO, interpretowany w świetle Karty, musi być zapewniony niezależnie od przepisu rozdziału V, na podstawie którego dokonywane jest przekazywanie danych osobowych do państwa trzeciego[15].

5. W wyroku w sprawie Schrems II Trybunał podkreślił obowiązek podmiotów przekazujących i podmiotów odbierających do zapewnienia, iż przetwarzanie danych osobowych odbywało się i będzie się nadal odbywało zgodnie ze stopniem ochrony przewidzianym w prawie UE w zakresie ochrony danych, do zawieszenia przekazywania danych czy też rozwiązania umowy w przypadku, gdy podmiot odbierający dane nie jest lub przestał być w stanie przestrzegać standardowych klauzul ochrony danych wprowadzonych do stosownej umowy zawartej między podmiotem przekazującym a podmiotem

[8] Art. 8 ust. 1 Karty praw podstawowych oraz art. 16 ust. 1 TFUE, preambuła 1, art. 1 ust. 2 RODO.
[9] Art. 52 ust. 1 Karty praw podstawowych UE.
[10] Motyw 4 RODO i C-507/17, Google LLC, następca prawny Google Inc., przeciwko Commission nationale de l'informatique et des libertés (CNIL), pkt 60.
[11] C-92/09 i C-93/02, Volker und Markus Schecke GbR przeciwko Land Hessen, opinia rzecznika generalnego E. Sharpston, 17 czerwca 2010 r., pkt 71.
[12] Art. 5 ust. 2 i art. 28 ust. 3 lit. h) RODO.
[13] Art. 44 i motyw 101 RODO, a także art. 47 ust. 2 lit. d) RODO.
[14] Wyrok TSUE z dnia 6 października 2015 r. Maximillian Schrems przeciwko Data Protection Commissioner, (dalej: C-362/14 (Schrems I)), pkt45.
[15] C-311/18 (Schrems II), pkt 92 i 93.

odbierającym[16]. Administrator lub podmiot przetwarzający działający jako podmiot przekazujący muszą zapewnić, że podmioty odbierające będą w stosownych przypadkach współpracować z podmiotem przekazującym w realizacji powyższych obowiązków, informując go np. o wszelkich zmianach wpływających na stopień ochrony otrzymanych danych osobowych w państwie podmiotu odbierającego[17]. Obowiązki te stanowią wyraz ustanowionej w RODO zasady rozliczalności w odniesieniu do przekazywania danych[18].

2 PLAN DZIAŁANIA: STOSOWANIE ZASADY ROZLICZALNOŚCI DO PRZEKAZYWANIA DANYCH W PRAKTYCE

6. Poniżej znaleźć można plan działań przedstawiający kroki, jakie należy podjąć, żeby dowiedzieć się, czy jako podmiot przekazujące dane muszą Państwo podjąć środki uzupełniające, aby móc zgodnie z prawem przekazywać dane poza EOG. Termin „Państwo" w niniejszym dokumencie odnosi się do administratora lub podmiotu przetwarzającego działających w roli podmiotu przekazującego, przetwarzającego dane osobowe w zakresie zastosowania RODO – w tym przetwarzania przez podmioty prywatne lub organy publiczne przy przekazywaniu danych do podmiotów prywatnych[19]. Jeśli chodzi o przekazywanie danych osobowych między organami publicznymi, konkretne wskazówki określono w Wytycznych 2/2020 w sprawie stosowania art. 46 ust. 2 lit. a) i art. 46 ust. 3 lit. b) rozporządzenia 2016/679 na potrzeby przekazywania danych osobowych między organami i podmiotami publicznymi z EOG i spoza EOG[20].

7. Dokonaną ocenę oraz podjęte i wdrożone środki uzupełniające należy odpowiednio dokumentować i udostępnić taką dokumentację na wniosek właściwego organu nadzorczego[21].

2.1 Krok 1: Rozpoznanie przeprowadzanych operacji przekazywania

8. Pierwszym krokiem, jaki należy wykonać, żeby dowiedzieć się o nałożonych na Państwo obowiązkach jako podmiotu przekazującego dane na potrzeby kontynuowania lub przeprowadzenia nowych operacji przekazywania danych osobowych[22], jest zapewnienie pełnej wiedzy o przeprowadzanych operacjach przekazywania (rozpoznanie przeprowadzanych operacji przekazywania). Rejestrowanie i zidentyfikowanie wszystkich operacji przetwarzania może być bardzo skomplikowanym przedsięwzięciem dla podmiotów zaangażowanych w liczne, zróżnicowane i regularne operacje przekazywania z państwami trzecimi i korzystających z usług szeregu podmiotów przetwarzających i podmiotów podprzetwarzających. Rozpoznanie przeprowadzanych operacji przekazywania jest koniecznym pierwszym etapem, żeby zrealizować Państwa obowiązki w ramach zasady rozliczalności.

[16] C-311/18 (Schrems II), pkt 134, 135, 139, 140, 141, 142.
[17] C-311/18 (Schrems II), pkt 134.
[18] Art. 5 ust. 2 i art. 28 ust. 3 lit. h) RODO.
[19] Zob. Wytyczne EROD 3/2018 w sprawie terytorialnego zakresu stosowania RODO (art. 3) https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_en
[20] Wytyczne EROD 2/2020 w sprawie stosowania art. 46 ust. 2 lit. a) i art. 46 ust. 3 lit. b) rozporządzenia 2016/679 na potrzeby przekazywania danych osobowych między organami i podmiotami publicznymi z EOG i spoza EOG; zob. https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-22020-articles-46-2-and-46-3-b_en
[21] Art. 5 ust. 2 RODO i art. 24 ust. 1 RODO.
[22] Należy zwrócić uwagę, że zdalny dostęp przez podmiot z państwa trzeciego do danych znajdujących się w EOG również uznawany jest za przekazywanie.

9. Aby w pełni rozpoznać przeprowadzane operacje przekazywania, mogą Państwo oprzeć się na rejestrach czynności przetwarzania, które mogą mieć Państwo obowiązek prowadzić jako administrator lub podmiot przetwarzający na podstawie art. 30 RODO[23]. Pomocne mogą okazać się także uprzednio przeprowadzone czynności zgodnie z art. 13 ust. 1 lit. f) i art. 14 ust. 1 lit. f) RODO dla celów powiadomienia osób, których dane dotyczą, o przekazywaniu ich danych osobowych do państw trzecich[24].

10. W procesie identyfikowania operacji przekazywania nie można zapominać o uwzględnieniu dalszego przekazywania, np. gdy Państwa podmioty przetwarzające spoza EOG przekazują powierzone im dane osobowe do podmiotów podprzetwarzających w innym lub tym samym państwie trzecim[25].

11. Zgodnie z zasadą „minimalizacji danych" na podstawie RODO[26] należy zweryfikować, czy wszystkie przekazywane dane są adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przekazywane do państwa trzeciego i tam przetwarzane.

12. Czynności tych należy dokonać przed przeprowadzeniem operacji przekazywania i aktualizować je przed ponownym podjęciem przekazywania po tym, jak zostało ono zawieszone: muszą Państwo wiedzieć, gdzie przekazane dane osobowe mogą się znajdować lub być przetwarzane przez podmioty odbierające (mapa miejsc przeznaczenia).

13. Należy pamiętać, że zdalny dostęp z państwa trzeciego (np. w sytuacji wsparcia) lub przechowywanie w chmurze zlokalizowanej poza EOG również uważa się za przekazywanie[27]. Innymi słowy, jeśli korzystają Państwo z międzynarodowej infrastruktury chmury, będą musieli Państwo ocenić, czy dane będą przekazywane do państw trzecich i do których, chyba że dostawca usług chmury wyraźnie stwierdzi w swojej umowie, że dane nie będą przetwarzane w państwach trzecich.

[23] Zob. art. 30 RODO, w szczególności ust. 1 lit. e) i ust. 2 lit. c). Ponadto prowadzone rejestry czynności przetwarzania powinny zawierać opis czynności przetwarzania, w tym m.in. kategorie osób, których dane dotyczą, kategorie danych i cele przetwarzania, a także konkretne informacje na temat operacji przetwarzania. Niektórzy administratorzy i niektóre podmioty przetwarzające są zwolnieni z obowiązku prowadzenia rejestrów czynności przetwarzania (art. 30 ust. 5 RODO). Dodatkowe informacje na temat powyższego zwolnienia można znaleźć w dokumencie Grupy Roboczej Artykułu 29 pt. „Position Paper on the derogations from the obligation to maintain records of processing activities pursuant to Article 30.5 GDPR" (dokument przedstawiający stanowisko w sprawie zwolnienia z obowiązku prowadzenia rejestru czynności przetwarzania na podstawie art. 30 ust. 5 RODO) (zatwierdzonym przez EROD dnia 25 maja 2018 r.).
[24] Zgodnie z zasadą przejrzystości na podstawie RODO należy poinformować osoby, których dane dotyczą, o przekazywaniu danych osobowych do państw trzecich (art. 13 ust. 1 lit. f) i art. 14 ust. 1 lit. f) RODO). Trzeba w szczególności powiadomić te osoby o stwierdzeniu lub braku stwierdzenia przez Komisję Europejską odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych. Informacje przekazane osobom, których dane dotyczą, muszą być prawidłowe i aktualne, zwłaszcza w świetle orzecznictwa Trybunału dotyczącego przekazywania.
[25] W przypadku, gdy administrator udzielił uprzedniej szczegółowej lub ogólnej pisemnej zgody zgodnie z art. 28 ust. 2 RODO.
[26] Art. 5 ust. 1 lit. c) RODO.
[27] Zob. Często zadawane pytanie nr 11: „należy pamiętać, że nawet udzielanie dostępu do danych z państwa trzeciego, np. w celach administracyjnych, również stanowi przekazanie danych", Często zadawane pytania EROD dotyczące wyroku Trybunału Sprawiedliwości Unii Europejskiej wydanego w sprawie C- 311/18 – Data Protection Commissioner przeciwko Facebook Ireland i Maximillianowi Schremsowi, z dnia 23 lipca 2020 r.

2.2 Krok 2: Określenie wykorzystywanych narzędzi przekazywania

14. Drugim koniecznym krokiem jest określenie, czy wykorzystywane narzędzia przekazywania, są wymienione i przewidziane w rozdziale V RODO.

Decyzje stwierdzające odpowiedni stopień ochrony

15. Komisja Europejska na podstawie **decyzji stwierdzającej odpowiedni stopień ochrony** dotyczącej niektórych lub wszystkich państw trzecich, do których przekazują Państwo dane, może uznać, że państwa takie zapewniają odpowiedni stopień ochrony danych osobowych[28].

16. Taka decyzja stwierdzająca odpowiedni stopień ochrony skutkuje tym, że możliwy jest przepływ danych osobowych z EOG do takiego państwa trzeciego bez konieczności zastosowania któregokolwiek z narzędzi przekazywania z art. 46 RODO.

17. Decyzja stwierdzająca odpowiedni stopień ochrony może odnosić się do całego państwa lub jego części. Decyzja taka może dotyczyć wszystkich operacji przekazywania danych do danego państwa lub ograniczać się do wybranych rodzajów przekazywania (np. w jednym sektorze)[29].

18. Komisja Europejska publikuje listę decyzji stwierdzających odpowiedni stopień ochrony na swojej stronie internetowej[30].

19. Jeśli przekazują Państwo dane osobowe do państw trzecich, regionów lub sektorów, których dotyczy decyzja Komisji Europejskiej stwierdzająca odpowiedni stopień ochrony (w stosownym zakresie), **nie ma potrzeby podejmowania jakichkolwiek dalszych kroków wskazanych w niniejszych zaleceniach**[31]. Konieczne będzie jednak nadal monitorowanie, czy decyzje stwierdzające odpowiedni stopień ochrony nie zostały uchylone lub unieważnione[32].

20. Należy pamiętać, że decyzje stwierdzające odpowiedni stopień ochrony nie uniemożliwiają osobom, których dane dotyczą, składania skarg. Nie stanowią one również przeszkody dla organów nadzorczych dla wniesienia sprawy do sądu krajowego w przypadku wątpliwości dotyczących ważności decyzji stwierdzającej odpowiedni stopień ochrony, żeby sąd krajowy mógł skierować odesłanie prejudycjalne mające doprowadzić do przeanalizowania tej ważności[33].

[28] Komisja Europejska władna jest określać na podstawie art. 45 RODO, czy dane państwo spoza UE zapewnia odpowiedni stopień ochrony danych. Komisja Europejska posiada również prawo do określenia, czy organizacja międzynarodowa zapewnia odpowiedni stopień ochrony.
[29] Art. 45 ust. 1 RODO.
[30] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en
[31] Pod warunkiem, że zarówno Państwo, jak i podmiot odbierający dane wdrożyliście środki mające na celu przestrzeganie innych zobowiązań na podstawie RODO; w przeciwnym wypadku takie środki należy wdrożyć.
[32] Komisja Europejska musi dokonywać okresowych przeglądów wszystkich decyzji stwierdzających odpowiedni stopień ochrony i monitorować, czy państwa trzecie, których takie decyzje dotyczą, nadal zapewniają odpowiedni stopień ochrony (zob. art. 45 ust. 3 i art. 45 ust. 4 RODO). Decyzje stwierdzające odpowiedni stopień ochrony mogą być także unieważnione przez TSUE (zob. wyroki w sprawach C-362/14 (Schrems I) i C-311/18 (Schrems II).
[33] C-311/18 (Schrems II), pkt 118 - 120. Organy nadzorcze nie mogą zignorować decyzji stwierdzającej odpowiedni stopień ochrony i zawiesić przekazywanie danych do takiego państwa lub zakazać go, powołując się wyłącznie na nieodpowiedni stopień ochrony. Mogą jedynie skorzystać ze swoich uprawnień do zawieszenia lub zakazania przekazywania danych osobowych do takiego państwa trzeciego na innej podstawie (np. niewystarczające środki bezpieczeństwa z naruszeniem art. 32 RODO czy też brak ważnej podstawy prawnej, na której bazuje przetwarzanie danych, z naruszeniem art. 6 RODO). Organy nadzorcze mogą zbadać w sposób całkowicie niezależny, czy przekazywanie tych danych spełnia wymogi ustanowione w RODO oraz, w odpowiednim

Przykład: Obywatel UE, Pan Schrems, w czerwcu 2013 r. wniósł do Irish Data Protection Commission (irlandzkiego komisarza ds. ochrony danych) skargę, w której zwrócił się o zawieszenie i zakazanie spółce Facebook Ireland przekazywania jego danych osobowych do Stanów Zjednoczonych; w tej skardze podniósł on, że prawo i praktyka obowiązujące w tym państwie nie zapewniają wystarczającej ochrony danych osobowych przechowywanych na jego terytorium przed działaniami nadzorczymi prowadzonymi przez władze publiczne. Data Protection Commission odrzuciła tę skargę w szczególności na tej podstawie, że w decyzji 2000/520 Komisja Europejska uznała, że w ramach programu „bezpiecznej przystani" Stany Zjednoczone zapewniają odpowiedni stopień ochrony przekazywanych danych osobowych. Pan Schrems zaskarżył decyzję Data Protection Commission i High Court (wysoki trybunał, Irlandia) zwrócił się do Trybunał Sprawiedliwości Unii Europejskiej (TSUE) z wnioskiem o wydanie orzeczenia w trybie prejudycjalnym w przedmiocie ważności decyzji 2000/520. Następnie TSUE unieważnił decyzję 2000/520 Komisji w sprawie adekwatności ochrony przewidzianej przez zasady ochrony prywatności w ramach bezpiecznej przystani[34].

Narzędzia przekazywania z art. 46 RODO

21. Art. 46 RODO wymienia szereg narzędzi przekazywania, cechujących się „odpowiednimi zabezpieczeniami", które podmioty przekazujące mogą wykorzystać dla celów przekazywania danych osobowych do państw trzecich w przypadku braku decyzji stwierdzających odpowiedni stopień ochrony. Główne rodzaje narzędzi przekazywania wymienione w art. 46 RODO są następujące:

- standardowe klauzule ochrony danych (SCC);
- wiążące reguły korporacyjne (WRK).
- kodeksy postępowania;
- mechanizmy certyfikacji;
- klauzule umowne *ad hoc*.

22. Niezależnie od wybranego narzędzia przekazywania wskazanego w art. 46 RODO, należy zapewnić, że zasadniczo przekazywane dane osobowe będą objęte merytorycznie równoważnym stopniem ochrony.

23. Narzędzia przekazywania wskazane w art. 46 RODO obejmują przede wszystkim odpowiednie zabezpieczenia o charakterze umownym, które mogą być stosowane w przypadku przekazywania danych do wszystkich państw trzecich. Sytuacja panująca w państwie trzecim, do którego dane są przekazywane, może jednak wymagać uzupełnienia tych narzędzi przekazywania i zawartych w nich zabezpieczeń dodatkowymi środkami („środkami uzupełniającymi") w celu zapewnienia merytorycznie równoważnego stopnia ochrony[35].

przypadku, mają możliwość wniesienia do sądów krajowych skargi mającej na celu skierowanie przez te sądy, jeśli podzielą one wątpliwości tego organu co do ważności tej decyzji Komisji stwierdzającej odpowiedni stopień ochrony, odesłania prejudycjalnego mającego doprowadzić do przeanalizowania tej ważności przez Trybunał Sprawiedliwości Unii Europejskiej.
[34] Sprawa C-362/14 (Schrems I).
[35] C-311/18 (Schrems II), pkt 130 i 133. Zob. również pkt 2.3 poniżej.

Wyjątki

24. W dodatku do decyzji stwierdzających odpowiedni stopień ochrony i narzędzi przekazywania z art. 46 RODO rozporządzenie przewiduje trzecią drogę dopuszczającą przekazywanie danych osobowych w określonych przypadkach. Z zastrzeżeniem podanych warunków możliwe będzie przekazanie danych osobowych na podstawie wyjątku wskazanego w art. 49 RODO.

25. Art. 49 GDPR ma wyjątkowy charakter. Zawarte w nim wyjątki muszą być interpretowane w sposób zawężający i odnosić się głównie do czynności przetwarzania, które są sporadyczne i niepowtarzające się. EROD wydała Wytyczne 2/2018 w sprawie wyjątków określonych w art. 49 rozporządzenia 2016/679.[36]

26. Przed skorzystaniem z któregokolwiek wyjątku przewidzianego w art. 49 RODO należy sprawdzić, czy przekazanie spełnia rygorystyczne wymogi, jakie zostały określone dla każdego z tych wyjątków.

***

27. Jeśli przekazanie danych nie może być w sposób zgodny z prawem oparte na decyzji stwierdzającej odpowiedni stopień ochrony ani na wyjątku z art. 49, należy przejść do Kroku 3.

2.3 Krok 3: Ocena, czy wykorzystywane narzędzie przekazywania z art. 46 RODO jest skuteczne w świetle wszystkich okoliczności przekazywania

28. Wykorzystanie narzędzia przekazywania z art. 46 RODO może okazać się niewystarczające. Takie narzędzie przekazywania musi bowiem zapewnić, że w wyniku przekazania nie dojdzie do uszczuplenia stopnia ochrony gwarantowanego na podstawie RODO[37]. Innymi słowy, narzędzie przekazywania musi być skuteczne w praktyce.

29. „Skuteczne" oznacza, że przekazane dane osobowe będą w państwie trzecim chronione w stopniu merytorycznie równoważnym temu gwarantowanemu w EOG[38]. Nie będzie mieć to miejsca, jeśli podmiot odbierający dane nie jest w stanie wywiązać się ze swoich zobowiązań wynikających z wybranego narzędzia przekazywania z art. 46 RODO ze względu na obowiązujące w państwie trzecim przepisy lub praktyki dotyczące przekazywania.

30. Należy zatem ocenić, w stosownych przypadkach we współpracy z podmiotem odbierającym, czy w prawie lub praktyce państwa trzeciego funkcjonuje cokolwiek, co w kontekście danej operacji przekazywania mogłoby negatywnie wpłynąć na skuteczność odpowiednich zabezpieczeń wykorzystywanych narzędzi przekazywania z art. 46 RODO. W stosownych przypadkach podmiot odbierający dane powinien przekazać właściwe źródła i informacje dotyczące państwa trzeciego, w którym prowadzi działalność gospodarczą, i przepisów mających zastosowanie do przekazywania. Można także odwołać się do innych źródeł informacji, wymienionych na zasadzie przykładu w załączniku 3[39].

[36] Dodatkowe informacje w tym zakresie znaleźć można pod adresem: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_en.
[37] Art. 44 RODO.
[38] C-311/18 (Schrems II), pkt 105 i drugie ustalenie.
[39] Zob. również pkt 43 poniżej.

31. Przeprowadzona ocena powinna uwzględnić wszystkie podmioty biorące udział w przekazaniu (np. administratorów, podmioty przetwarzające, podmioty podprzetwarzające w państwie trzecim), które zidentyfikowano w wyniku mapowania operacji przekazywania. Im więcej uczestniczących administratorów, podmiotów przetwarzających i podmiotów odbierających, tym bardziej złożona będzie ta ocena. Trzeba także wziąć pod uwagę dalsze przekazanie, jakie może mieć miejsce.

32. W tym celu należy zapoznać się z charakterystyką każdej przeprowadzanej operacji przekazywania i ustalić, w jaki sposób porządek prawny panujący w państwie, do którego dane są przekazywane (lub przekazywane dalej), stosuje się do takiego przekazywania.

33. Stosowny kontekst prawny będzie zależeć od okoliczności przekazywania, w szczególności od:

    - celów, w jakich dane są przekazywane i przetwarzane (np. marketing, HR, przechowywanie, wsparcie informatyczne, badania kliniczne);
    - rodzajów podmiotów zaangażowanych w przetwarzanie (prywatne czy publiczne; administrator czy podmiot przetwarzający);
    - sektora, w którym przekazywanie ma miejsce (np. adtech, telekomunikacja, sektor finansowy itd.);
    - kategorii przekazywanych danych osobowych (np. dane osobowe dotyczące dzieci mogą być objęte zakresem stosowania przepisów szczególnych w państwie trzecim);
    - tego, czy dane będą przechowywane w państwie trzecim i czy do danych przechowywanych w UE/EOG możliwy będzie tylko dostęp zdalny;
    - formatu danych, które będą przekazywane (tj. czy dane będą w formie zwykłego tekstu, spseudonimizowane lub zaszyfrowane[40]);
    - możliwości dalszego przekazywania danych z jednego państwa trzeciego do innego państwa trzeciego[41].

34. Należy ocenić, czy którykolwiek z obowiązujących przepisów może negatywnie wpłynąć na zobowiązania zawarte w wybranym narzędziu przekazywania z art. 46 RODO. Konieczna będzie weryfikacja, czy zobowiązania, dzięki którym osoby, których dane dotyczą, mogą w praktyce skutecznie wykonać swoje prawa w kontekście międzynarodowego przekazania danych (takie jak wnioski u udostępnienie, sprostowanie lub usunięcie przekazywanych danych), nie są niwelowane przez przepisy w docelowym państwie trzecim.

35. Trzeba również ocenić stosowne przepisy o charakterze ogólnym w takim zakresie, w jakim wpływają one na skuteczne stosowanie zabezpieczeń zawartych w narzędziach przekazywania z art. 46 RODO i na prawa podstawowe osób fizycznych (w szczególności prawo do środka zaskarżenia przyznane osobie, której dane dotyczą, w przypadku dostępu organów publicznych państwa trzeciego do przekazywanych danych).

36. W każdym przypadku należy zwrócić szczególną uwagę na odpowiednie przepisy, w tym przepisy określające wymogi udostępnienia danych osobowych organom publicznym lub przyznające takim organom publicznym prawo dostępu do danych osobowych (np. dla celów egzekwowania prawa karnego, nadzoru regulacyjnego i bezpieczeństwa narodowego). Jeżeli te wymogi lub uprawnienia są

[40] Niektóre państwa trzecie nie zezwalają na odbieranie zaszyfrowanych danych.
[41] W przypadku, gdy administrator udzielił uprzedniej szczegółowej lub ogólnej pisemnej zgody zgodnie z art. 28 ust. 2 RODO.

ograniczone do tego, co jest niezbędne i proporcjonalne w demokratycznym społeczeństwie[42], nie mogą one negatywnie wpływać na zobowiązania zawarte w wybranym narzędziu przekazywania z art. 46 RODO.

37. Normy UE, takie jak art. 47 i 52 Karty praw podstawowych Unii Europejskiej, należy stosować jako punkt odniesienia w celu oceny, czy taki dostęp przez organy publiczne jest ograniczony do tego, co jest niezbędne i proporcjonalne w demokratycznym społeczeństwie, oraz czy osobom, których dane dotyczą, zapewnia się skuteczne środki zaskarżenia.

38. Przy przeprowadzaniu tej oceny istotne mogą być również inne aspekty systemu prawa tego państwa trzeciego, np. czynniki wymienione w art. 45 ust. 2 RODO[43]. Przykładowo, sytuacja praworządności w państwie trzecim może mieć znaczenie dla oceny skuteczności zapewnionych osobom fizycznym mechanizmów zaskarżenia (do sądu) bezprawnego dostępu organów rządowych do danych osobowych. Istnienie kompleksowego prawa ochrony danych lub niezależnego urzędu ochrony danych, a także przestrzeganie międzynarodowych instrumentów przewidujących zabezpieczenia danych, może przyczynić się do zapewnienia proporcjonalności ingerencji rządu[44].

***

39. Zalecenia EROD w sprawie niezbędnych gwarancji europejskich wskazują elementy, które należy ocenić w celu ustalenia, czy ramy prawne państwa trzeciego dotyczące dostępu władz publicznych, tzn. krajowych służb bezpieczeństwa i organów ścigania, do danych osobowych, uznać można za uzasadnioną ingerencję (nie naruszającą zobowiązań podjętych w ramach narzędzi przekazywania z art. 46 RODO). W szczególności należy dokładnie rozważyć, czy przepisy dotyczące dostępu organów publicznych do danych są niejednoznaczne lub nie są publicznie dostępne.

40. W przypadku operacji przekazywania danych przy wykorzystaniu narzędzi przekazywania z art. 46 zalecenia EROD w sprawie niezbędnych gwarancji europejskich mogą dać wskazówki podmiotowi przekazującemu dane i podmiotowi odbierającemu dane na potrzeby oceny, czy takie uprawnienia w nieuzasadniony sposób ingerują w obowiązek podmiotu odbierającego dane do zapewnienia niezbędnej równoważności.

41. Brak merytorycznie równoważnego stopnia ochrony będzie szczególnie widoczny w przypadku, gdy przepisy lub praktyka państwa trzeciego znajdujące zastosowanie do danej operacji przetwarzania nie spełniają wymogów wynikających z niezbędnych gwarancji europejskich.

[42] Zob. art. 47 i 52 Karty praw podstawowych Unii Europejskiej, art. 23 ust. 1 RODO i zalecenia EROD 02/2020 w sprawie niezbędnych gwarancji europejskich dla środków nadzoru, 10 listopada 2020 r., https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en.
[43] C-311/18 (Schrems II), pkt 104.
[44] Dla przykładu: Konwencja Nr 108 Rady Europy (Konwencja o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, ETS nr 108) lub Konwencja nr 108+ Rady Europy (Protokół zmieniający Konwencję o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, CETS nr 223) zapewniają egzekwowalne, międzynarodowe środki zaskarżenia w przypadku naruszenia ochrony danych i przyczyniają się do zapewnienia minimalnego stopnia ochrony danych osobowych i poszanowania życia prywatnego.

42. Ocena musi być oparta przede wszystkim na publicznie dostępnych przepisach. Niekiedy może się to jednak okazać niewystarczające, ponieważ prawo państwa trzeciego może zawierać braki. W takiej sytuacji, jeśli nadal planują Państwo przekazanie danych, należy przyjrzeć się innym istotnym i obiektywnym czynnikom[45], a nie polegać na czynnikach subiektywnych, takich jak prawdopodobieństwo, że organy publiczne uzyskają dostęp do danych w sposób niezgodny z normami UE. Ocenę tę należy przeprowadzić z należytą starannością i dokładnie ją udokumentować, jako że podmiot będzie rozliczany z decyzji, jaką może podjąć na tej podstawie[46].

43. Ocenę można uzupełnić informacjami uzyskanymi z innych źródeł[47], takimi jak:

- czynniki dowodzące na podstawie zgłoszonych precedensów, przepisów i praktyki, że organ państwa trzeciego będzie domagał się dostępu do danych za wiedzą podmiotu odbierającego dane lub bez niej;
- czynniki dowodzące na podstawie zgłoszonych precedensów, uprawnień oraz zasobów technicznych, finansowych i ludzkich, którymi dysponuje, że organ państwa trzeciego będzie mógł uzyskać dostęp do danych za pośrednictwem podmiotu odbierającego dane lub drogą bezpośredniego przechwycenia kanału komunikacji.

44. Przeprowadzona ocena może ostatecznie wykazać, że wykorzystywane narzędzie przekazywania z art. 46 RODO wraz z właściwymi mu odpowiednimi zabezpieczeniami:

- skutecznie zapewnia, że przekazane dane osobowe objęte są stopniem ochrony w państwie trzecim, który jest merytorycznie równoważny temu gwarantowanemu w EOG. Przepisy i praktyki państwa trzeciego znajdujące zastosowanie do danej operacji przekazywania umożliwiają podmiotowi odbierającemu realizację zobowiązań wynikających z wybranego narzędzia przekazywania. Ocenę należy przeprowadzić ponownie w stosownych odstępach czasu lub w razie, gdy wystąpią istotne zmiany (zob. krok 6).
- nie zapewnia w sposób skuteczny merytorycznie równoważnego stopnia ochrony. Podmiot odbierający dane nie może spełnić leżących na nim zobowiązań ze względu na przepisy lub praktyki państwa trzeciego znajdujące zastosowanie do danej operacji przekazywania. TSUE podkreślił, że w przypadku, gdy narzędzia przekazywania z art. 46 RODO okażą się niewystarczające, obowiązkiem podmiotu przekazującego dane jest wdrożenie skutecznych środków uzupełniających lub zaniechanie przekazania danych osobowych[48].

[45] Zob. pkt 43 poniżej, a także załącznik 3.
[46] Art. 5 ust. 2 RODO.
[47] Zob. także załącznik 3.
[48] C-311/18 (Schrems II), pkt 134-135.

TSUE orzekł na przykład, że art. 702 FISA nie zapewnia minimalnych wymogów wynikających z zasady proporcjonalności na podstawie prawa UE, w związku z czym nie można uznać, że jest ograniczony do tego, co jest ściśle niezbędne. Oznacza to, że stopień ochrony programów zatwierdzonych na podstawie art. 702 FISA nie jest merytorycznie równoważny zabezpieczeniom wymaganym na podstawie prawa UE. W konsekwencji jeśli podmiot odbierający dane lub jakikolwiek dalszy odbiorca, któremu podmiot odbierające dane może udostępnić dane, podlega art. 702 FISA[49], na potrzeby danej operacji przekazywania będzie można wykorzystać standardowe klauzule ochrony danych lub inne narzędzia przekazywania z art. 46 RODO pod warunkiem, że dodatkowe, uzupełniające środki techniczne sprawiają, że dostęp do przekazanych danych będzie niemożliwy lub nieskuteczny.

2.4 Krok 4: Przyjęcie środków uzupełniających

45. Jeśli ocena przeprowadzona w kroku 3 wykazała, że wybrane narzędzie przekazywania z art. 46 RODO nie jest skuteczne, konieczne będzie rozważenie, w stosownych przypadkach we współpracy z podmiotem odbierającym dane, czy dostępne są jakiekolwiek środki uzupełniające, które po dodaniu do zabezpieczeń zawartych już w narzędziach przekazywania mogłyby zapewnić, że przekazywane dane są objęte w państwie trzecim stopniem ochrony merytorycznie równoważnym temu gwarantowanemu w UE[50]. „Środki uzupełniające" z definicji mają charakter uzupełniający w stosunku do zabezpieczeń zawartych już w narzędziach przekazywania z art. 46 RODO[51].

46. Należy określić w każdym konkretnym przypadku, które środki uzupełniające mogłyby okazać się skuteczne w odniesieniu do zestawu operacji przekazywania do danego państwa trzeciego przy wykorzystaniu konkretnego narzędzia przekazywania z art. 46 RODO. Można oprzeć się na wynikach poprzednich ocen (z kroków 1, 2 i 3 powyżej) w celu sprawdzenia potencjalnej skuteczności środków uzupełniających w zakresie zagwarantowania wymaganego stopnia ochrony.

47. Co do zasady środki uzupełniające mają charakter umowny, techniczny lub organizacyjny. Połączenie różnych środków w taki sposób, że będą się one wzajemnie wspierać i uzupełniać, może doprowadzić do zwiększenia stopnia ochrony i przyczynić się do osiągnięcia standardów unijnych.

48. Same środki umowne i organizacyjne nie będą w większości przypadków w stanie rozwiązać problemu dostępu organów publicznych państwa trzeciego do danych osobowych (w przypadku, gdy dostęp taki w nieuzasadniony sposób ingeruje w zobowiązanie podmiotu odbierającego dane do zapewnienia równoważności stopnia ochrony). W rzeczy samej pojawią się sytuacje, gdy jedynie środki techniczne będą mogły ograniczyć lub uniemożliwić dostęp organów publicznych państwa trzeciego do danych osobowych, w szczególności dla celów nadzoru[52]. W takich przypadkach środki umowne lub organizacyjne mogą uzupełniać środki techniczne i wzmacniać ogólny stopień ochrony danych, np. tworząc przeszkody dla prób uzyskania przez organy publiczne dostępu do danych w sposób, który nie jest zgodny ze standardami UE.

49. W stosownych przypadkach we współpracy z podmiotem odbierającym dane można odwołać się do poniższej niewyczerpującej listy czynników, aby określić, które środki uzupełniające byłyby najbardziej skuteczne w ochronie przekazywanych danych:

    - format danych, które będą przekazywane (tj. w formie zwykłego tekstu, spseudonimizowanego lub zaszyfrowanego);
    - charakter danych;
    - długość i złożoność procesu przetwarzania danych, liczba podmiotów uczestniczących w przetwarzaniu i relacje między nimi (np. czy przekazywanie obejmuje wielu administratorów i wiele podmiotów przetwarzających, czy też udział podmiotów przetwarzających, które będą przekazywać otrzymane dane do podmiotu odbierającego dane (uwzględniając stosowne przepisy znajdujące zastosowanie do nich na podstawie prawa państwa trzeciego przeznaczenia));[53]
    - możliwość dalszego przekazywania danych w ramach danego państwa trzeciego lub nawet do innych państw trzecich (np. zaangażowanie podmiotów podprzetwarzających podmiotu odbierającego dane[54]).

Przykłady środków uzupełniających

50. Wybrane przykłady środków technicznych, umownych i organizacyjnych, które można rozważyć, podane zostały w niewyczerpującym wykazie zawartym w załączniku 2.

***

51. Jeśli wdrożono skuteczne środki uzupełniające, które w połączeniu z wybranym narzędzie przekazywania z art. 46 RODO, osiągają stopień ochrony merytorycznie równoważny temu zagwarantowanemu w EOG, operacja przekazywania może się odbyć.

[49] Art. 702 FISA znajduje zastosowanie, jeśli dane zostały uzyskane „od lub przy pomocy dostawcy usług łączności elektronicznej" (art. 702 FISA = 50 USC § 1881a, lit. h) pkt 2 ppkt A tiret (vi)), który z kolei zdefiniowany jest w 50 USC § 1881 lit. b) pkt 4) jako
„(A) operator telekomunikacyjny zgodnie z definicją w sekcji 153 tytułu 47;
(B) dostawca usług łączności elektronicznej zgodnie z definicją w sekcji 2510 tytułu 18;
(C) dostawca zdalnych usług obliczeniowych zgodnie z definicją w sekcji 2711 tytułu 18;
(D) każdy inny dostawca usług łączności, który ma dostęp do usług łączności przewodowej lub elektronicznej podczas przekazywania lub przechowywania takich informacji; lub
(E) członek kadry zarządzającej, pracownik lub przedstawiciel podmiotu, o którym mowa w podpunktach (A), (B), (C) lub (D)".

[50] C-311/18 (Schrems II), pkt 96.

[51] Motyw 109 RODO i C-311/18 (Schrems II), pkt 133.

[52] W przypadku gdy taki dostęp wykracza poza to, co jest niezbędne i proporcjonalne w demokratycznym społeczeństwie; zob. art. 47 i 52 Karty praw podstawowych Unii Europejskiej, art. 23 ust. 1 RODO i zalecenia EROD 02/2020 w sprawie niezbędnych gwarancji europejskich dla środków nadzoru, 10 listopada 2020 r., https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en .

[53] RODO nakłada na administratorów i podmioty przetwarzające różne obowiązki. Przekazywanie może mieć miejsce od administratora do administratora, pomiędzy współadministratorami, od administratora do podmiotu przetwarzającego oraz – pod warunkiem uzyskania zgody administratora – od podmiotu przetwarzającego do administratora i od podmiotu przetwarzającego do podmiotu przetwarzającego.

[54] Zob. przypis 25.

52. Jeśli jednak nie znaleziono lub nie wdrożono skutecznego środka uzupełniającego, który by zapewnił, że przekazywane dane osobowe cieszą się merytorycznie równoważnym stopniem ochrony[55], nie wolno rozpoczynać przekazywania danych osobowych do danego państwa trzeciego przy wykorzystaniu narzędzia przekazywania z art. 46 RODO. Jeśli operacja przekazywania już ma miejsce, należy zawiesić lub zakończyć przekazywanie danych osobowych[56] . Zgodnie z zabezpieczeniami zawartymi w wykorzystywanym narzędziu przekazywania z art. 46 RODO dane, które już zostały przekazane do takiego państwa trzeciego, oraz ich kopie powinny zostać zwrócone lub zniszczone w całości przez podmiot odbierający dane[57].

Przykład: prawo państwa trzeciego zakazuje określonych środków uzupełniających (np. szyfrowania) lub w inny sposób niweczy ich skuteczność. W takim wypadku nie można rozpocząć przekazywania danych osobowych lub należy wstrzymać dalsze przekazywanie do tego państwa.

53. Jeśli podjęta zostanie decyzja o kontynuowania przekazywania mimo tego, że podmiot odbierający nie jest w stanie wywiązać się z zobowiązań wynikających z narzędzia przekazywania z art. 46 RODO, należy powiadomić właściwy organ nadzorczy zgodnie ze szczegółowymi przepisami dotyczącymi danego narzędzia przekazywania z art. 46 RODO[58]. Właściwy organ nadzorczy zawiesi przekazywanie danych lub zakaże go, gdy uzna, że nie można zapewnić merytorycznie równoważnego stopnia ochrony[59].

54. Właściwy organ nadzorczy może zastosować wszelkie inne środki naprawcze (np. nałożyć grzywnę), gdy przekazywanie zostanie rozpoczęte lub będzie kontynuowane mimo tego, że nie można udowodnić merytorycznie równoważnego stopnia ochrony w państwie trzecim.

2.5 Krok 5: Podjęcie kroków proceduralnych w przypadku, gdy zidentyfikowano skuteczne środki uzupełniające

55. Proceduralne kroki, które być może będzie trzeba podjąć, gdy zidentyfikowano skuteczne środki uzupełniające do wdrożenia, mogą się różnić w zależności od wykorzystywanego lub planowanego do wykorzystania narzędzia przekazywania z art. 46 RODO.

2.5.1 Standardowe klauzule ochrony danych („SCC") (art. 46 ust. 2 lit. c) i d) RODO)

56. Jeśli zamierzają Państwo wprowadzić środki uzupełniające w dodatku do standardowych klauzul umownych, nie ma potrzeby składania wniosku do właściwego organu nadzorczego o pozwolenia na dodanie tego rodzaju klauzul lub dodatkowych zabezpieczeń, o ile określone środki uzupełniające nie są w bezpośredniej lub pośredniej sprzeczności ze standardowymi klauzulami umownymi i są

[55] W przypadku gdy taki dostęp wykracza poza to, co jest niezbędne i proporcjonalne w demokratycznym społeczeństwie; zob. art. 47 i 52 Karty praw podstawowych Unii Europejskiej, art. 23 ust. 1 RODO i zalecenia EROD 02/2020 w sprawie niezbędnych gwarancji europejskich dla środków nadzoru, 10 listopada 2020 r., https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en .

[56] C-311/18 (Schrems II), pkt 135.

[57] Zob. klauzulę 12 w załączniku do decyzji Komisji 87/2010 w sprawie standardowych klauzul umownych; zob. (dobrowolną) dodatkową klauzulę o wypowiedzeniu w załączniku B do decyzji Komisji 2004/915/WE w zakresie wprowadzenia alternatywnego zestawu standardowych klauzul umownych.

[58] Zob. Często zadawane pytania dotyczące wyroku Trybunału Sprawiedliwości Unii Europejskiej wydanego w sprawie C-311/18 – Data Protection Commissioner przeciwko Facebook Ireland i Maximillianowi Schremsowi, przyjęte dnia 23 lipca 2020 r., w szczególności pytanie nr 5, 6 i 9. Zob. klauzulę 4 lit. g) decyzji Komisji 2010/87/UE, jak również klauzulę 5 lit. a) decyzji Komisji 2001/497/WE i załącznik – Pakiet II klauzula II lit. c) decyzji Komisji 2004/915/WE.

[59] C-311/18 (Schrems II), pkt 113 i 121.

wystarczające, żeby zapewnić, iż stopień ochrony gwarantowany przez RODO nie ulegnie uszczupleniu[60]. Podmiot przekazujący i podmiot odbierający muszą zapewnić, że takie dodatkowe klauzule nie będą mogły być zinterpretowane w sposób ograniczający prawa i obowiązki wskazane w standardowych klauzulach umownych ani w żaden inny sposób obniżający stopień ochrony danych. Muszą być Państwo w stanie wykazać powyższe, w tym jednoznaczność wszystkich klauzul, zgodnie z zasadą rozliczalności i obowiązkiem zapewnienia wystarczającego stopnia ochrony. Właściwy organ nadzorczy ma w razie potrzeby prawo do przeglądu tych uzupełniających klauzul (np. w przypadku skargi lub dochodzenia wszczętego z własnej inicjatywy).

57. W przypadku gdy zamierzają Państwo zmienić same standardowe klauzule ochrony danych lub jeżeli dodane środki uzupełniające pozostają w bezpośredniej lub pośredniej sprzeczności ze standardowymi klauzulami umownymi, uznaje się, że nie opierają się już Państwo na standardowych klauzulach umownych[61], w związku z czym należy wystąpić o zezwolenie właściwego organu nadzorczego zgodnie z art. 46 ust. 3 lit. a) RODO.

2.5.2 Wiążące reguły korporacyjne (art. 46 ust. 2 lit. b) RODO)

58. Tok rozumowania wskazany w wyroku w sprawie Schrems II stosuje się również do innych narzędzi przekazywania z art. 46 ust. 2 RODO, jako że wszystkie te narzędzia mają charakter zasadniczo umowny, w związku z czym gwarancje przewidziane i zobowiązania przyjęte przez ich strony nie mogą być wiążące dla organów publicznych państwa trzeciego[62].

59. Wyrok w sprawie Schrems II znajduje zastosowanie do przekazywania danych osobowych na podstawie wiążących reguł korporacyjnych, ponieważ przepisy państwa trzeciego mogą mieć wpływ na ochronę zapewnianą przez takie narzędzia. Nadal trwają dyskusję dotyczące dokładnego wpływu wyroku w sprawie Schrems II na wiążące reguły korporacyjne. EROD w najkrótszym możliwym terminie przekaże bardziej szczegółowe informacje na temat tego, czy konieczne może być uwzględnienie w wiążących regułach korporacyjnych dodatkowych zobowiązań zgodnie z listami referencyjnymi WP256/257.[63]

[60] Motyw 109 RODO stanowi: „Możliwość korzystania przez administratora lub podmiot przetwarzający ze standardowych klauzul ochrony danych przyjętych przez Komisję lub organ nadzorczy nie powinna stanowić dla administratora lub podmiotu przetwarzającego przeszkody, by standardowe klauzule ochrony danych włączyć do szerszej umowy, takiej jak umowa między wspomnianym podmiotem przetwarzającym a innym podmiotem przetwarzającym, ani by dodać inne klauzule lub dodatkowe zabezpieczenia, pod warunkiem że nie są one bezpośrednio lub pośrednio sprzeczne ze standardowymi klauzulami umownymi przyjętymi przez Komisję lub organ nadzorczy ani nie naruszają podstawowych praw lub wolności osób, których dane dotyczą". Podobne postanowienia zawarte są w standardowych klauzulach umownych przyjętych przez Komisję Europejską na mocy dyrektywy 95/45/WE.

[61] Zob. analogicznie przyjętą już Opinię 17/2020 EROD w sprawie projektu standardowych klauzul umownych przedłożonego przez organ nadzorczy Słowenii (art. 28 ust. 8 RODO), która zawiera podobne postanowienie („Ponadto Rada przypomina, że możliwość stosowania standardowych klauzul umownych przyjętych przez organ nadzorczy nie uniemożliwia stronom dodawania innych klauzul lub dodatkowych gwarancji, pod warunkiem że nie są one sprzeczne, bezpośrednio lub pośrednio z przyjętymi standardowymi klauzulami umownymi, ani nie naruszają podstawowych praw i wolności osób, których dane dotyczą. Dodatkowo, w przypadku zmiany standardowych klauzul ochrony danych, strony nie będą dłużej uznawane za podmioty, które wdrożyły standardowe klauzule umowne"), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinion_202017_art28sccs_si_en.pd .

[62] CJEU, C-311/18 (Schrems II), pkt 132.

[63] Grupa Robocza Art. 29, Dokument roboczy ustanawiający tabelę zawierającą elementy i zasady, które mają zostać uwzględnione w wiążących regułach korporacyjnych, ostatnio zmieniony i przyjęty w dniu 6 lutego 2018

60. Trybunał podkreślił, że obowiązkiem podmiotu przekazującego dane i podmiotu odbierającego dane jest dokonanie oceny, czy poziom ochrony wymagany prawem Unii jest przestrzegany w danym państwie trzecim, co pozwoli ustalić, czy gwarancje przewidziane w standardowych klauzulach umownych lub wiążących regułach korporacyjnych mogą być przestrzegane w praktyce. Jeżeli tak nie jest, należy ocenić, czy możliwe jest zastosowanie dodatkowych środków w celu zapewnienia merytorycznie równoważnego stopnia ochrony do tego przewidzianego w EOG, jak również, czy prawo lub praktyka państwa trzeciego nie wpłynie niekorzystnie na takie dodatkowe środki w taki sposób, że pozbawi je skuteczności.

2.5.3 Klauzule umowne *ad hoc* (art. 46 ust. 3 lit. a) RODO)

61. Tok rozumowania wskazany w wyroku w sprawie Schrems II stosuje się również do innych narzędzi przekazywania z art. 46 ust. 2 RODO, jako że wszystkie te narzędzia mają charakter zasadniczo umowny, w związku z czym gwarancje przewidziane i zobowiązania przyjęte przez ich strony nie mogą być wiążące dla organów publicznych państwa trzeciego[64]. Wyrok w sprawie Schrems II znajduje zatem zastosowanie do przekazywania danych osobowych na podstawie klauzul umownych *ad hoc*, ponieważ przepisy państwa trzeciego mogą mieć wpływ na ochronę zapewnianą przez takie narzędzia. Nadal trwają dyskusję dotyczące dokładnego wpływu wyroku w sprawie Schrems II na klauzule umowne *ad hoc*. EROD w najkrótszym możliwym terminie przekaże bardziej szczegółowe informacje na ten temat.

2.6 Krok 6: Ponowna ocena w odpowiednich odstępach czasu

62. Należy na bieżąco monitorować, w stosownych przypadkach we współpracy z podmiotami odbierającymi dane, zmiany w państwie trzecim, do którego dane osobowe są przekazywane, jakie mogą mieć wpływ na dokonaną uprzednio ocenę stopnia ochrony i na decyzje, które podjęto na jej podstawie w związku z przekazywaniem. Rozliczalność jest obowiązkiem o charakterze ciągłym (art. 5 ust. 2 RODO).

63. Zaleca się wdrożenie dostatecznie solidnych mechanizmów w celu zapewnienia, że przekazywanie można natychmiast zawiesić lub zakończyć, jeśli:

- podmiot odbierający naruszył zobowiązania, jakie podjął na podstawie narzędzia przekazywania z art. 46 RODO, lub nie jest w stanie spełnić tych zobowiązań; lub
- środki uzupełniający utraciły swoją skuteczność w takim państwie trzecim.

r., WP 256 rev.01; Grupa Robocza Art. 29, Dokument roboczy ustanawiający tabelę zawierającą elementy i zasady, które mają zostać uwzględnione w wiążących regułach korporacyjnych, ostatnio zmieniony i przyjęty w dniu 6 lutego 2018 r., WP 257 rev.01.

[64] CJEU, C-311/18 (Schrems II), pkt 132.

3 WNIOSKI

64. RODO ustanawia zasady dotyczące przetwarzania danych osobowych w EOG, umożliwiając w ten sposób swobodny przepływ danych osobowych na terytorium EOG. Rozdział V RODO reguluje przekazywanie danych osobowych do państw trzecich i stawia wysoko poprzeczkę: przekazywanie nie może naruszać stopnia ochrony osób fizycznych zagwarantowanego w RODO (art. 44 RODO). Wyrok TSUE w sprawie C-311/18 (Schrems II) podkreśla potrzebę zapewnienia ciągłości stopnia ochrony gwarantowanej na podstawie RODO w odniesieniu do danych osobowych przekazywanych do państwa trzeciego[65].

65. W celu zapewnienia merytorycznie równoważnego stopnia ochrony danych konieczne jest przede wszystkim dokładne rozpoznanie przeprowadzanych operacji przekazywania. Należy zweryfikować, czy przekazywane dane są adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przekazywane i przetwarzane w państwie trzecim.

66. Trzeba również określić wykorzystywane narzędzie przekazywania. Jeśli nie jest ono objęte decyzją stwierdzającą odpowiedni stopień ochrony, należy sprawdzić w każdym konkretnym przypadku, czy prawo lub praktyka państwa trzeciego przeznaczenia nie narusza zabezpieczeń zawartych w narzędziu przekazywania z art. 46 RODO w kontekście przeprowadzanych operacji przekazywania. W przypadku gdy samo narzędzie przekazywania z art. 46 RODO nie zapewnia merytorycznie równoważnego stopnia ochrony przekazywanych danych osobowych, lukę tę wypełnić mogą środki uzupełniające.

67. Jeśli znalezienie lub wdrożenie środków uzupełniających, które zapewniałyby, że przekazywane dane osobowe objęte są merytorycznie równoważnym stopniem ochrony, nie jest możliwe, nie wolno rozpocząć operacji przekazywania danych osobowych do takiego państwa trzeciego przy wykorzystaniu wybranego narzędzia przekazywania. Jeśli operacja przekazywania już się rozpoczęła, są Państwo zobowiązani natychmiast zawiesić lub zakończyć przekazywanie danych osobowych.

68. Właściwy organ nadzorczy ma prawo do zawieszenia lub zakończenia przekazywania danych osobowych do państwa trzeciego, jeśli nie zapewniono ochrony przekazywanych danych, jaka wymagana jest na podstawie prawa UE, w szczególności art. 45 i 46 RODO oraz Karty praw podstawowych.

W imieniu Europejskiej Rady Ochrony Danych

Przewodnicząca

(Andrea Jelinek)

[65] C-311/18 (Schrems II), pkt 93.

ZAŁĄCZNIK 1: DEFINICJE

- „Państwo trzecie" oznacza każde państwo niebędące państwem członkowskim EOG.
- „EOG" oznacza Europejski Obszar Gospodarczy i obejmuje państwa członkowskie Unii Europejskiej, a także Islandię, Norwegię i Liechtenstein. RODO stosuje się do tych trzech ostatnich państw na mocy Porozumienia o EOG, w szczególności Załącznika XI i Protokołu 37 do tego porozumienia.
- „RODO" oznacza Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).
- „Karta" oznacza Kartę praw podstawowych Unii Europejskiej, Dz.U. C 326 z 26.10.2012, s. 391–407.
- „TSUE" lub „Trybunał" oznacza Trybunał Sprawiedliwości Unii Europejskiej. Jest on organem sądowym Unii Europejskiej, który we współpracy z sądami i trybunałami państw członkowskich zapewnia jednolite stosowanie i jednolitą wykładnię prawa UE.
- „Podmiot przekazujący dane" oznacza administratora lub podmiot przetwarzający w EOG, który przekazuje dane osobowe administratorowi lub podmiotowi przetwarzającemu w państwie trzecim.
- „Podmiot odbierający dane" oznacza administratora lub podmiot przetwarzający w państwie trzecim, który otrzymuje dane osobowe przekazywane z EOG lub uzyskuje do nich dostęp.
- „Narzędzie przekazywania z art. 46" odnosi się do odpowiednich zabezpieczeń na podstawie art. 46 RODO, jakie podmioty przekazujące dane mają obowiązek zastosować przy przekazywaniu danych osobowych do państwa trzeciego w razie braku decyzji stwierdzającej odpowiedni stopień ochrony zgodnie z art. 45 ust. 3 RODO. Art. 46 ust. 2 i ust. 3 RODO zawierają listę narzędzi przekazywania z art. 46, z których administratorzy lub podmioty przetwarzające mogą korzystać.
- „SCC" oznacza standardowe klauzule ochrony danych (lub standardowe klauzule umowne) przyjęte przez Komisję Europejską dla potrzeb przekazywania danych między administratorami i podmiotami przetwarzającymi w EOG a administratorami i podmiotami przetwarzającymi spoza EOG. Standardowe klauzule umowne przyjęte przez Komisję Europejską stanowią narzędzie przekazywania na podstawie RODO, zgodnie z art. 46 ust. 2 lit. c) i art. 46 ust. 5 RODO.

ZAŁĄCZNIK 2: PRZYKŁADY ŚRODKÓW UZUPEŁNIAJĄCYCH

69. Poniżej wskazano przykładowe środki uzupełniające, jakie można uwzględnić, jeśli dojdą Państwo do Kroku 4 „Przyjęcie środków uzupełniających". Lista ta nie jest wyczerpująca. Wybór i wdrożenie jednego z lub kilku tych środków nie zapewni w sposób pewny i systematyczny, że przeprowadzona operacja przekazywania spełni standard merytorycznie równoważnego stopnia ochrony wymaganego na podstawie prawa UE. Należy wybrać te środki uzupełniające, które mogą skutecznie zagwarantować taki stopień ochrony w odniesieniu do przeprowadzanych operacji przekazywania.

70. Dany środek uzupełniający uznać można za skuteczny w rozumieniu wyroku TSUE w sprawie Schrems II, jeśli prowadzi on – i w zakresie, w jakim prowadzi on – do usunięcia konkretnych uchybień określonych w wyniku przeprowadzonej oceny sytuacji prawnej w państwie trzecim. Jeśli ostatecznie nie będzie możliwe zapewnienie merytorycznie równoważnego stopnia ochrony, przekazywanie danych nie może mieć miejsca.

71. Jako administrator lub podmiot przetwarzający mogą być Państwo już zobowiązani do wdrożenia niektórych środków opisanych w niniejszym załączniku, nawet jeśli podmiot odbierający, z którego usług Państwo korzystają, objęty jest decyzją stwierdzającą odpowiedni stopień ochrony, podobnie jak mogą być Państwo zobowiązani do ich wdrożenia podczas przetwarzania danych w ramach EOG[66].

Środki techniczne

72. W niniejszej sekcji wskazano w sposób niewyczerpujący przykładowe środki techniczne, które mogą uzupełniać zabezpieczenia zawarte w narzędziach przekazywania z art. 46 RODO w celu zapewnienia przestrzegania wymaganego przez prawo UE stopnia ochrony w kontekście przekazywania danych osobowych do państwa trzeciego. Środki te będą konieczne zwłaszcza wtedy, gdy przepisy państwa trzeciego nakładają na podmiot odbierający dane wymagania, które są sprzeczne z zabezpieczeniami zawartymi w narzędziach przekazywania z art. 46 RODO i które w szczególności mogą mieć negatywny wpływ na udzielone umownie gwarancje merytorycznie równoważnego stopnia ochrony przed dostępem organów władz publicznych tego państwa trzeciego do tych danych[67].

73. W celu osiągnięcia jeszcze większej jasności niniejsza sekcja najpierw określi środki techniczne, które mogą być potencjalnie skuteczne w pewnych okolicznościach/scenariuszach w zapewnianiu merytorycznie równoważnego stopnia ochrony. W następnej kolejności opisane zostaną okoliczności/scenariusze, dla których nie znaleziono żadnego środka technicznego zapewniającego taki stopień ochrony.

Scenariusze, dla których znaleziono *skuteczne* środki

74. Środki wymienione poniżej mają na celu zagwarantować, że dostęp organów publicznych państw trzecich do przekazywanych danych nie wpływa negatywnie na skuteczność odpowiednich zabezpieczeń zawartych w narzędziach przekazywania z art. 46 RODO. Środki te znajdują zastosowanie nawet wtedy, gdy dostęp organów publicznych dokonany jest z poszanowaniem prawa państwa

[66] Art. 5 ust. 2 RODO, art. 32 RODO.
[67] C-311/18 (Schrems II), pkt 135.

podmiotu odbierającego, jeśli dostęp tego rodzaju wykracza poza to, co jest niezbędne i proporcjonalne w społeczeństwie demokratycznym[68]. Ich celem jest zapobieganie potencjalnym naruszeniom w zakresie dostępu poprzez uniemożliwienie organom określenia osób, których dane dotyczą, wywnioskowania informacji na ich temat, odnalezienia ich w innym kontekście lub powiązania przekazywanych danych z innymi zestawami danych będących w posiadaniu tych organów, a które mogą obejmować m.in. identyfikatory internetowe generowane przez urządzenia, aplikacje, narzędzia i protokoły, jakie osoby, których dane dotyczą, wykorzystują w innych kontekstach.

75. Organy publiczne państw trzecich mogą podejmować starania, żeby uzyskać dostęp do przekazywanych danych:

a) w tranzycie poprzez dostęp do kanałów komunikacji wykorzystywanych do przekazywania danych do państwa otrzymującego. Dostęp ten może przyjąć formę bierną, kiedy treści komunikatu, czasem po przeprowadzeniu procesu selekcji, zostaną po prostu skopiowane. Dostęp może być jednak również bardziej czynny w takim znaczeniu, że organy publiczne przejmą proces łączności, nie tylko czytając komunikat, ale także manipulując lub zatajając jego części;

b) przechowywanych przez zamierzonego odbiorcę poprzez uzyskanie dostępu do samych zakładów przetwarzania lub poprzez nałożenie na odbiorcę danych obowiązku zlokalizowania i ekstrakcji istotnych danych oraz przekazania ich do władz.

76. Niniejsza sekcja uwzględnia przypadki, gdy zastosowano środki skuteczne w obu tych scenariuszach. Różne środki uzupełniające mogą być wykorzystywane i wystarczające w okolicznościach danej operacji przetwarzania, jeśli przepisy państwa otrzymującego przewidują tylko jedną formę dostępu. Podmiot przekazujący dane musi zatem dokładnie przeanalizować, przy wsparciu podmiotu odbierającego dane, jakie obowiązki nałożono na podmiot odbierający dane.

Dla przykładu amerykańskie podmioty odbierające dane, o których mowa w 50 USC § 1881a (art. 702 FISA), mają bezpośredni obowiązek zapewnić dostęp do odebranych danych osobowych będących w ich posiadaniu, przechowywanych przez nich lub znajdujących się pod ich kontrolą oraz przekazać takie dane do władz. Może to dotyczyć również kluczy kryptograficznych służących do odszyfrowania danych.

77. Scenariusze opisują konkretne okoliczności i podjęte środki. Wszelkie zmiany do scenariuszy mogą doprowadzić do odmiennych wniosków.

78. Administratorzy być może będą musieli zastosować niektóre lub wszystkie opisane tutaj środki niezależnie od stopnia ochrony przewidzianego przez przepisy obowiązujące podmiot odbierający dane, ponieważ mają oni obowiązek spełnienia wymogów na nich nałożonych na podstawie art. 25 i 32 RODO w konkretnych okolicznościach, w jakich dochodzi do przekazywania. Innymi słowy, podmioty przekazujące mogą być zobowiązane do wdrożenia środków opisanych w tym dokumencie, nawet jeśli podmiot odbierający, z którego usług korzystają, objęty jest decyzją stwierdzającą odpowiedni stopień ochrony, podobnie jak administratorzy i podmioty przetwarzające mogą być zobowiązani do ich wdrożenia podczas przetwarzania danych w ramach EOG.

[68] Zob. art. 47 i 52 Karty praw podstawowych Unii Europejskiej, art. 23 ust. 1 RODO i zalecenia EROD w sprawie niezbędnych gwarancji europejskich dla środków nadzoru.

Scenariusz nr 1: Przechowywanie danych w celach wykonania kopii zapasowej i w innych celach, które nie wymagają dostępu do niezakodowanych danych

79. Podmiot przekazujące dane korzysta z usług dostawcy usług hostingowych w państwie trzecim w celu przechowywania danych osobowych, np. na potrzeby kopii zapasowej.

Jeżeli

1. dane osobowe są przetwarzane przy wykorzystaniu mocnego szyfrowania przed wysyłaniem,
2. algorytm szyfrowania i jego parametryzacja (np. długość klucza, tryb działania, jeśli dotyczy) są zgodne z aktualnym stanem wiedzy i można je uznać za zaawansowaną ochronę przed analizą kryptograficzną przeprowadzaną przez organy publiczne w państwie otrzymującym, uwzględniając dostępne tym organom zasoby i środki techniczne (np. moc obliczeniową na potrzeby ataków brute-force),
3. siła szyfrowania uwzględnia okres, przez jaki należy zachować poufność zaszyfrowanych danych osobowych,
4. algorytm szyfrowania jest perfekcyjnie wdrażany przez odpowiednio aktualizowane programy, których zgodność ze specyfikacją wybranego algorytmu została potwierdzona, np. w formie certyfikacji,
5. klucze są odpowiednio zarządzane (generowane, przydzielane, przechowywane, w razie konieczności powiązane z tożsamością docelowego odbiorcy i blokowane), oraz
6. klucze są przechowywane wyłącznie pod kontrolą podmiotu przekazującego dane lub innych podmiotów, którym powierzono to zadanie, mających siedzibę w EOG lub państwie trzecim, na terytorium lub w określonym sektorze lub określonych sektorach w państwie trzecim, bądź organizacji międzynarodowej, w stosunku do których Komisja zgodnie z art. 45 RODO stwierdziła, że zapewniają odpowiedni stopień ochrony,

EROD uznaje, że przeprowadzone operacje szyfrowania stanowią skuteczny środek uzupełniający.

Scenariusz nr 2: Przekazywanie danych spseudonimizowanych

80. Podmiot przekazujący dane najpierw pseudonimizuje posiadane dane, a następnie przekazuje je do państwa trzeciego w celach analizy, np. na potrzeby badań.

Jeżeli

1. podmiot przekazujący dane przekazuje dane osobowe przetworzone w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, ani wykorzystać w celu odnalezienia osoby, której dane dotyczą, w ramach większej grupy, bez użycia dodatkowych informacji[69],
2. takie dodatkowe informacje znajdują się w wyłącznym posiadaniu podmiotu przekazującego dane i przechowywane są osobno w państwie członkowskim lub w państwie trzecim, terytorium, określonym sektorze lub określonych sektorach w państwie trzecim, bądź organizacji międzynarodowej, w stosunku do których Komisja zgodnie z art. 45 RODO stwierdziła, że zapewniają odpowiedni stopień ochrony,

[69] Zgodnie z art. 4 ust. 5 RODO: „Pseudonimizacja" oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.

3. ujawnienie lub nieupoważnione wykorzystanie takich dodatkowych informacji nie jest możliwe ze względu na odpowiednie zabezpieczenia techniczne i organizacyjne i zapewniono, że podmiot przekazujący dane zachowuje wyłączną kontrolę nad algorytmem lub archiwum umożliwiającymi ponowną identyfikację przy wykorzystaniu dodatkowych informacji, oraz
4. administrator, przeprowadziwszy dogłębną analizę określonych danych przy uwzględnieniu wszelkich informacji, jakie mogą znajdować się w posiadaniu organów publicznych państwa otrzymującego, ustalił, że nie można przypisać spseudonimizowanych danych osobowych zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, nawet po przeprowadzeniu porównania z takimi informacjami,

EROD uznaje, że przeprowadzona pseudonimizacja stanowi skuteczny środek uzupełniający.

81. Należy zwrócić uwagę, że w wielu przypadkach czynniki określające fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej, jej lokalizację lub korzystanie z usług internetowych w określonym czasie[70] mogą umożliwić identyfikację takiej osoby, nawet jeśli pomięto jej nazwisko, adres czy inne zwykłe identyfikatory.

82. Odnosi się to przede wszystkim do przypadków, gdy dane dotyczą wykorzystania usług informacyjnych (data dostępu, kolejność użytych funkcji, charakterystyka użytego sprzętu itd.). Usługi te mogą równie dobrze podlegać, podobnie jak podmiot odbierający dane osobowe, obowiązkowi przyznania dostępu tym samym organom publicznym w ich jurysdykcji, które z dużym prawdopodobieństwem będą wtedy posiadać dane o wykorzystaniu tych usług informacyjnych przez osobę docelową.

83. Ponadto, zważywszy, że wykorzystanie niektórych usług informacyjnych ma charakter publiczny, i uwzględniając możliwość ich wykorzystania przez podmioty posiadające znaczne zasoby, administratorzy będą musieli zachować szczególną ostrożność, biorąc pod uwagę, że organy publiczne w ich jurysdykcji z dużym prawdopodobieństwem posiadają dane o wykorzystaniu usług informacyjnych przez osobę docelową.

Scenariusz nr 3: Zaszyfrowane dane jedynie przechodzą przez państwo trzecie

84. Podmiot przekazujący dane chce przekazać dane do państwa docelowego uznanego za gwarantujące odpowiednią ochronę zgodnie z art. 45 RODO. Dane przesyłane są przez państwo trzecie.

Jeżeli

1. podmiot przekazujący dane przekazuje dane osobowe do podmiotu odbierającego dane w jurysdykcji zapewniającej odpowiednią ochronę, a dane są przesyłane przez internet i mogą geograficznie przechodzić przez państwo trzecie, które nie zapewnia merytorycznie równoważnego stopnia ochrony,
2. zastosowano szyfrowanie transmisji i zapewniono, że protokoły szyfrowania są najnowocześniejsze i zapewniają skuteczną ochronę przeciwko aktywnym i pasywnym atakom za pomocą zasobów, o których wiadomo, że są dostępne dla organów publicznych państwa trzeciego,
3. odszyfrowanie możliwe jest tylko poza danym państwem trzecim,

[70] Art. 4 ust. 1 RODO: „Dane osobowe" oznaczają wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej (osoba, której dane dotyczą); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora, takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

4. podmioty zaangażowane w proces komunikacji wspólnie wybiorą wiarygodny organ lub infrastrukturę certyfikacji klucza publicznego,
5. wykorzystano konkretne najnowocześniejsze środki ochronne przeciwko aktywnym i pasywnym atakom na zaszyfrowaną transmisję,
6. w przypadku gdy szyfrowanie transmisji samo przez się nie zapewnia odpowiedniego bezpieczeństwa ze względu na wcześniejsze przypadki podatności infrastruktury lub wykorzystanego oprogramowania, dane osobowe zaszyfrowano na całej drodze przesyłu danych na warstwie aplikacji dzięki zastosowaniu najnowocześniejszych metod szyfrowania,
7. algorytm szyfrowania i jego parametryzacja (np. długość klucza, tryb działania, jeśli dotyczy) są zgodne z aktualnym stanem wiedzy i można je uznać za zaawansowaną ochronę przed analizą kryptograficzną przeprowadzoną przez organy publiczne w państwie tranzytu, uwzględniając dostępne tym organom zasoby i środki techniczne (np. moc obliczeniową na potrzeby ataków brute-force),
8. siła szyfrowania uwzględnia okres, przez jaki należy zachować poufność zaszyfrowanych danych osobowych,
9. algorytm szyfrowania jest perfekcyjnie wdrażany przez odpowiednio aktualizowane programy, których zgodność ze specyfikacją wybranego algorytmu została potwierdzona, np. w formie certyfikacji,
10. wykluczono istnienie luk (backdoor) w oprogramowaniu i sprzęcie,
11. klucze są odpowiednio zarządzane (generowane, przydzielane, przechowywane, w razie konieczności powiązane z tożsamością docelowego odbiorcy i blokowane), przez podmiot przekazujący lub inny zaufany podmiot podmiotu przekazującego działający w jurysdykcji oferującej merytorycznie równoważny stopień ochrony,

EROD uznaje, że szyfrowanie transmisji, w razie konieczności w połączeniu z szyfrowaniem na całej drodze przesyłu danych, stanowi skuteczny środek uzupełniający.

Scenariusz nr 4: Chroniony odbiorca

85. Podmiot przekazujący dane przekazuje dane osobowe do podmiotu odbierającego dane w państwie trzecim, podlegającego szczególnej ochronie na podstawie przepisów tego państwa, np. w celu wspólnego świadczenia usług medycznych dla pacjenta lub usług prawnych dla klienta.

Jeżeli

1. przepisy państwa trzeciego zwalniają będący rezydentem podmiot odbierający z potencjalnego naruszenia dostępu do danych posiadanych przez tego odbiorcę we wskazanym celu, np. na podstawie obowiązku zachowania tajemnicy zawodowej, który stosuje się do podmiotu odbierającego dane,
2. takie zwolnienie dotyczy wszystkich informacji posiadanych przez podmiot odbierający dane, które mogą być wykorzystane w celu obejścia ochrony informacji uprzywilejowanych (klucze kryptograficzne, hasła, inne dane uwierzytelniające itp.),
3. podmiot odbierający dane nie korzysta z usług podmiotu przetwarzającego w takim zakresie, który umożliwiłby organom publicznym uzyskanie dostępu do danych, kiedy znajdują się one w posiadaniu podmiotu przekazującego, ani podmiot odbierający dane nie przekazuje danych innemu podmiotowi, który nie podlega ochronie na podstawie narzędzi przekazywania z art. 46 RODO,

4. dane osobowe zostały przed wysyłką zaszyfrowane metodą zgodną z najnowocześniejszymi rozwiązaniami i gwarantującą, że odszyfrowanie nie będzie możliwe bez znajomości klucza do deszyfrowania (szyfrowanie na całej drodze przesyłu danych) przez cały okres, kiedy dane muszą być chronione,
5. klucz do deszyfrowania jest na wyłącznym przechowaniu chronionego podmiotu odbierającego dane i jest należycie zabezpieczony środkami technicznymi i organizacyjnymi zgodnymi z najnowocześniejszymi rozwiązaniami przed nieupoważnionym wykorzystaniem lub ujawnieniem, oraz
6. podmiot przekazujący dane w sposób wiarygodny ustalił, że klucz do szyfrowania, z którego zamierza skorzystać, odpowiada kluczowi do deszyfrowania znajdującemu się w posiadaniu odbiorcy,

EROD uznaje, że wykonane szyfrowanie transmisji stanowi skuteczny środek uzupełniający.

Scenariusz nr 5: Przetwarzanie dzielone lub przetwarzanie przez wiele podmiotów

86. Podmiot przekazujący dane chce, żeby dane były przetwarzane łącznie przez co najmniej dwa niezależne podmioty przetwarzające mające siedziby w dwóch różnych jurysdykcjach, bez jednoczesnego ujawnienia im treści danych. Przed transmisją dzieli dane w taki sposób, że żadna z części otrzymanych przez podmioty przetwarzające nie wystarcza do odtworzenia danych osobowych w części lub całości. Podmiot przekazujący dane otrzymuje wyniki przetwarzania w sposób niezależny od każdego z podmiotów przetwarzających i łączy otrzymane części, tworząc w ten sposób końcowy rezultat, który może stanowić dane osobowe lub dane zagregowane.

Jeżeli

1. podmiot przekazujący dane przetwarza dane osobowe w taki sposób, że dzieli je na dwie lub więcej części, które nie mogą zostać zinterpretowane lub przypisane do konkretnej osoby, której dane dotyczą, bez wykorzystania dodatkowych informacji,
2. każda z części przekazana zostaje do innych podmiotów przetwarzających, które mają siedziby w różnych jurysdykcjach,
3. podmioty przetwarzające mogą przetwarzać dane wspólnie, np. w przy wykorzystaniu obliczeń wielopodmiotowych, w taki sposób, że żadne informacje nie zostają ujawnione któremukolwiek z tych podmiotów, za wyjątkiem tych informacji, które podmioty te posiadały przed obliczeniem,
4. algorytm wykorzystywany na potrzeby wspólnych obliczeń jest zabezpieczony przed aktywnymi agresorami,
5. nie ma dowodów na współpracę między organami publicznymi zlokalizowanymi w odpowiednich jurysdykcjach, w których siedziby mają podmioty przetwarzające, co dałoby im dostęp do wszystkich zestawów danych osobowych znajdujących się w posiadaniu podmiotów przetwarzających i pozwoliłoby im na odtworzenie i wykorzystanie treści danych osobowych w czystej postaci w przypadku, gdy takie wykorzystanie naruszyłoby istotę podstawowych praw i wolności osób, których dane dotyczą. Podobnie organy publiczne któregokolwiek z państw nie powinny mieć prawa dostępu do danych osobowych znajdujących się w posiadaniu podmiotów przetwarzających we wszystkich właściwych jurysdykcjach.
6. administrator, przeprowadziwszy dogłębną analizę określonych danych przy uwzględnieniu wszelkich informacji, jakie mogą znajdować się w posiadaniu organów publicznych państw otrzymujących, ustalił, że nie można przypisać żadnej części danych osobowych, jakie przekazywane są przez niego podmiotom przetwarzającym, zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, nawet po przeprowadzeniu porównania z takimi informacjami,

EROD uznaje, że przetwarzanie dzielone stanowi skuteczny środek uzupełniający.

Scenariusze, w których nie znaleziono *skutecznego* środka

87. Środki opisane poniżej w określonych okolicznościach nie zapewniałyby w skuteczny sposób merytorycznie równoważnego stopnia ochrony danych przekazywanych do państwa trzeciego. Z tego względu nie można by ich uznać za środki uzupełniające.

Scenariusz nr 6: Przekazanie do dostawców usług chmury obliczeniowej lub innych podmiotów przetwarzających, wymagające dostępu do niezakodowanych danych

88. Podmiot przekazujący dane korzysta z usług dostawcy chmury obliczeniowej lub innych podmiotów przetwarzających w celu przetworzenia danych osobowych w państwie trzecim zgodnie z otrzymanymi instrukcjami.

Jeżeli

1. administrator przekazuje dane do dostawcy chmury obliczeniowej lub innego podmiotu przetwarzającego,
2. dostawca usług chmury lub inny podmiot przetwarzający potrzebuje dostępu do niezakodowanych danych na potrzeby realizacji powierzonego zadania, oraz
3. uprawnienia przyznane organom publicznym państwa otrzymującego w zakresie dostępu do przekazywanych danych wykraczają poza to, co niezbędne i proporcjonalne w demokratycznym społeczeństwie[71],

EROD, uwzględniając obecny stan wiedzy, nie jest w stanie przewidzieć skutecznego środka technicznego, dzięki któremu taki dostęp nie naruszałby praw osób, których dane dotyczą. EROD nie wyklucza, że dalszy rozwój technologiczny może zapewnić środki, które osiągną zamierzony cel biznesowy, i nie będą wymagać dostępu do niezakodowanych danych.

89. W takim scenariuszu, gdy niezaszyfrowane dane osobowe są technicznie konieczne podmiotowi przetwarzającemu do świadczenia usług, szyfrowanie transmisji i szyfrowanie danych w spoczynku, nawet zastosowane jednocześnie, nie stanowią środka uzupełniającego, który zapewniałby merytorycznie równoważny stopień ochrony, jeśli podmiot odbierający dane jest w posiadaniu kluczy kryptograficznych.

Scenariusz nr 7: Dostęp zdalny do danych w celach biznesowych

90. Podmiot przekazujący dane udostępnia dane osobowe podmiotom w państwie trzecim na potrzeby realizacji wspólnych celów biznesowych. Typowy układ może obejmować mających siedzibę w państwie członkowskim administratora lub podmiot przetwarzający, które przekazują dane osobowe administratorowi lub podmiotowi przetwarzającemu w państwie trzecim, w ramach tej samej grupy przedsiębiorstw, lub grupę przedsiębiorstw prowadzących wspólną działalność gospodarczą. Podmiot odbierający dane może przykładowo wykorzystać dane, jakie otrzyma, żeby świadczyć na rzecz

[71] Zob. art. 47 i 52 Karty praw podstawowych Unii Europejskiej, art. 23 ust. 1 RODO i zalecenia EROD w sprawie niezbędnych gwarancji europejskich dla środków nadzoru.

podmiotu przekazującego dane profesjonalne usługi kadrowe, do których potrzebuje danych dotyczących zasobów ludzkich, albo żeby prowadzić komunikację telefoniczną lub e-mailową z klientami podmiotu przekazującego dane, którzy mieszkają w Unii Europejskiej.

Jeżeli

1. podmiot przekazujący dane przekazuje dane podmiotowi odbierającemu dane w państwie trzecim, udostępniając je w powszechnie wykorzystywanym systemie informacyjnym w sposób, dzięki któremu podmiot odbierający będzie mógł uzyskać bezpośredni dostęp do danych wedle jego wyboru, albo przekazując je bezpośrednio pojedynczo lub masowo przy wykorzystaniu usług łączności,
2. podmiot odbierający wykorzystuje niezakodowane dane na własne potrzeby,
3. uprawnienia przyznane organom publicznym państwa otrzymującego w zakresie dostępu do przekazywanych danych wykraczają poza to, co niezbędne i proporcjonalne w demokratycznym społeczeństwie,

EROD nie jest w stanie przewidzieć skutecznego środka technicznego, dzięki któremu taki dostęp nie naruszałby praw osób, których dane dotyczą.

91. W takim scenariuszu, gdy niezaszyfrowane dane osobowe są technicznie konieczne podmiotowi przetwarzającemu do świadczenia usług, szyfrowanie transmisji i szyfrowanie danych w spoczynku, nawet zastosowane jednocześnie, nie stanowią środka uzupełniającego, który zapewniałby merytorycznie równoważny stopień ochrony, jeśli podmiot odbierający dane jest w posiadaniu kluczy kryptograficznych.

Dodatkowe środki umowne

92. Środki te zasadniczo obejmują zobowiązania umowne[72] o charakterze jednostronnym, dwustronnym lub wielostronnym[73]. W przypadku wykorzystania narzędzia przekazywania z art. 46 RODO narzędzie takie będzie w większości przypadków już obejmować pewne zobowiązania (przede wszystkim o charakterze umownym) podejmowane przez podmiot przekazujący dane i podmiot odbierający dany, pełniące funkcję zabezpieczeń danych osobowych[74].

93. W niektórych wypadkach środki te mogą uzupełniać i wzmacniać zabezpieczenia wynikające z narzędzia przekazywania i właściwych przepisów państwa trzeciego, gdy, uwzględniając okoliczności przekazywania, te narzędzia i przepisy nie spełniają wszystkich warunków wymaganych do zapewnienia stopnia ochrony merytorycznie równoważnego temu gwarantowanemu w UE. W świetle charakteru środków umownych, które zasadniczo nie są w stanie wiązać władz takiego państwa trzeciego, gdy nie są one stronami umowy[75], środki te należy połączyć z innymi środkami technicznymi i organizacyjnymi, żeby zapewnić wymagany stopień ochrony. Wybór i wdrożenie jednego z lub kilku

[72] Np. w ramach wiążących reguł korporacyjnych, które w każdym przypadku powinny regulować niektóre ze środków wskazanych poniżej.

[73] Będą mieć prywatny charakter i nie będą uważane za umowy międzynarodowe na podstawie prawa międzynarodowego publicznego. Nie będą w związku z tym wiązać organów publicznych państwa trzeciego, bowiem nie są one stronami tej umowy zawartej między prywatnymi podmiotami w państwach trzecich, jak Trybunał podkreślił w swoim wyroku w sprawie C-311/18 (Schrems II), pkt 125.

[74] Zob. wyrok w sprawie C-311/18 (Schrems II), pkt 137 w którym Trybunał uznał, że SCC przewidują „skuteczne mechanizmy umożliwiające w praktyce zapewnienie przestrzegania wymaganego przez prawo Unii stopnia ochrony i czy odbywające się na podstawie takich klauzul przekazywanie danych osobowych zostanie w przypadku ich naruszenia lub niemożności ich przestrzegania zawieszone lub zakazane", zob. także pkt 148).

[75] C-311/18 (Schrems II), pkt 125.

tych środków nie zapewni w sposób pewny i systematyczny, że przeprowadzona operacja przekazywania spełni standard merytorycznie równoważnego stopnia ochrony wymaganego na podstawie prawa UE.

94. W zależności od tego, jakie środki umowne zawarte są już w wykorzystywanym narzędziu przekazywania z art. 46 RODO, pomocne mogą okazać się również dodatkowe środki umowne, dzięki którym posiadające siedzibę w EOG podmioty przekazujące dane dowiedzą się o nowych rozwiązaniach mających wpływ na ochronę danych przekazywanych do państw trzecich.

95. Jak wskazano powyżej, środki umowne nie będą w stanie wyłączyć stosowania przepisów państwa trzeciego niespełniających standardów niezbędnych gwarancji europejskich EROD w przypadku, gdy przepisy te nakładają na podmioty odbierające dane obowiązek stosowania się do nakazów od organów publicznych[76].

96. Poniżej znaleźć można przykładowe potencjalne środki umowne, pogrupowane zgodnie z ich charakterem:

Nałożenie obowiązku umownego do stosowania określonych środków technicznych

97. ***W zależności od konkretnych okoliczności danej operacji przekazywania umowa może przewidywać, że na potrzeby przekazywania należy wprowadzić określone środki techniczne (patrz powyżej proponowane środki techniczne).***

98. ***Warunki skuteczności:***

- Klauzula ta może być skuteczna w sytuacji, gdy podmiot przekazujący stwierdził potrzebę zastosowania środków technicznych. Należy nadać jej formę prawną, żeby zapewnić, iż podmiot odbierający również zobowiąże się do wprowadzenia koniecznych środków technicznych.

Obowiązki w zakresie przejrzystości:

99. ***Podmiot przekazujący może uzupełnić umowę załącznikami zawierającymi informacje przekazane przez podmiot odbierający wedle jego najlepszych starań dotyczące dostępu do danych przez organy publiczne, w tym w dziedzinie wywiadu, pod warunkiem że przepisy w państwie docelowym są zgodne z niezbędnymi gwarancjami europejskimi EROD. Może to pomóc podmiotowi przekazującemu dane wywiązać się ze swojego obowiązku udokumentowania oceny stopnia ochrony w państwie trzecim.***

100. Przykładowo, podmiot odbierający może być zobowiązany do:

(1) określenia przepisów i regulacji w państwie docelowym, znajdujących zastosowanie do podmiotu odbierającego lub jego (dalszych) podmiotów przetwarzających, które dają prawo organom publicznym do dostępu do przekazywanych danych osobowych, w szczególności w dziedzinie wywiadu, egzekwowania prawa oraz nadzoru administracyjnego i regulacyjnego w odniesieniu do przekazywanych danych;

[76] Wyrok TSUE w sprawie C-311/18 (Schrems II), pkt 132.

(2) w braku przepisów regulujących dostęp organów publicznych do danych, podania informacji i danych statystycznych, w oparciu o doświadczenia podmiotu odbierającego lub raporty z różnych źródeł (np. od partnerów, z otwartych źródeł, krajowego orzecznictwa i decyzji krajowych wydanych przez organy nadzoru), dotyczących dostępu organów publicznych do danych osobowych w sytuacjach analogicznych do okoliczności danej operacji przekazywania danych (tj. w określonym obszarze regulacyjnym; w odniesieniu do rodzaju podmiotów, do których należy podmiot odbierający dane itd.);
(3) wskazania podjętych środków dla celu uniemożliwienia dostępu do przekazywanych danych (jeśli dotyczy);
(4) podania dostatecznie szczegółowych informacji o wszystkich otrzymanych przez podmiot odbierający w określonym czasie[77] żądaniach dostępu organów publicznych do danych osobowych, w szczególności w obszarach wymienionych w podpunkcie (1) powyżej, w tym informacji o otrzymanych żądaniach, żądanych danych, organie, który wysunął żądanie, podstawie prawnej ujawnienia i zakresie, w jakim podmiot odbierający ujawnił żądane dane[78];
(5) określenia, czy i w jakim zakresie podmiot odbierający ma prawny zakaz przekazania informacji wymienionych w podpunktach (1) – (5) powyżej.

101. Informację tę można przekazać w formie ustrukturyzowanych kwestionariuszy, które podmiot odbierający wypełni i podpisze, z zastrzeżeniem zobowiązania umownego podmiotu odbierającego do zadeklarowania w określonym terminie wszelkich możliwych zmian w odniesieniu do tych informacji, zgodnie z obowiązującą praktyką w zakresie procesów należytej staranności.

102. ***Warunki skuteczności:***

- Podmiot odbierający musi być w stanie przekazać, wedle swojej najlepszej wiedzy i dołożywszy należytej staranności w celu ich uzyskania, podmiotowi przekazującemu informacje tego rodzaju[79].
- Obowiązek ten nałożony na podmiot odbierający służy zapewnieniu, iż podmiot przekazujący będzie w każdym czasie wiedział o zagrożeniach, z jakimi wiąże się przekazywanie danych do państwa trzeciego. Pozwoli on zatem podmiotowi przekazującemu odstąpić od zawarcia umowy lub w przypadku zmian informacji po jej zawarciu spełnić obowiązek zawieszenia operacji przekazywania lub rozwiązania umowy, jeśli przepisy państwa trzeciego, zabezpieczenia zawarte w narzędziu przekazywania z art. 46 RODO i wszelkie dodatkowe zabezpieczenia, które zostały wdrożone, nie są już w stanie zapewnić stopnia ochrony merytorycznie równoważnego temu gwarantowanemu w UE. Obowiązek ten nie może jednak uzasadnić ujawnienia danych osobowych przez podmiot odbierający ani dawać podstaw do oczekiwania, że nie będzie dalszych żądań dostępu.

***

[77] Długość okresu powinna zależeć od poziomu zagrożenia dla praw i wolności osób, których dane są przekazywane, np. ostatni rok przed zakończeniem używania narzędzia przekazywania danych przez podmiot przekazujący dane
[78] Wywiązanie się z tego obowiązku samo przez się nie oznacza zapewnienia odpowiedniego stopnia ochrony. Jednocześnie niewłaściwe ujawnienie, które miało miejsce, prowadzi do konieczności podjęcia środków uzupełniających.
[79] Zob. pkt 32.5 powyżej.

103. ***Podmiot przekazujący może również dodać klauzulę, zgodnie z którą podmiot odbierający oświadczy, iż 1) nie stworzył celowo luk typu back door lub podobnych rozwiązań programistycznych, które mogłyby być wykorzystane w celu uzyskania dostępu do systemu lub danych osobowych, (2) nie stworzył celowo ani nie zmienił procesów biznesowych w taki sposób, który umożliwiłby dostęp do systemu lub danych osobowych, i 3) że prawo krajowe lub polityka państwowa nie wymagają od podmiotu odbierającego stworzenia lub utrzymania luk typu back door ani umożliwienia dostępu do danych osobowych lub systemów, ani nie wymagają od podmiotu odbierającego posiadania lub przekazania klucza do szyfrowania[80].***

104. ***Warunki skuteczności:***

- Istnienie przepisów lub polityki państwowej, które uniemożliwiają podmiotom odbierającym ujawnienie informacji, może sprawić, że klauzula ta będzie nieskuteczna. Podmiot odbierający być może nie będzie mógł zatem zawrzeć umowy lub będzie musiał powiadomić podmiot przekazujący o braku możliwości dalszej realizacji swoich zobowiązań umownych[81].
- Umowa musi przewidywać kary lub prawo podmiotu przekazującego do rozwiązania umowy z krótkim wyprzedzeniem w przypadku, gdy podmiot odbierający nie powiadomi o istnieniu luki typu back door czy podobnego rozwiązania programistycznego, zmanipulowanych procesach biznesowych lub wymogu wprowadzenia powyższych lub nie powiadomi podmiotu przekazującego niezwłocznie po tym, jak dowie się o istnieniu powyższych.

***

105. ***Podmiot przekazujący może wzmocnić swoje uprawnienie do przeprowadzenia audytu[82] lub inspekcji urządzeń przetwarzania danych podmiotu odbierającego, na miejscu lub zdalnie, w celu weryfikacji, czy dane zostały ujawnione organom publicznym i na jakich warunkach (dostęp niewykraczający poza to, co niezbędne i proporcjonalne w demokratycznym społeczeństwie), np. poprzez zawiadomienie z krótkim wyprzedzeniem, wprowadzenie mechanizmów zapewniających niezwłoczne działanie organów kontrolujących czy wzmocnienie autonomii podmiotu przekazującego w zakresie wyboru organu kontrolującego.***

106. ***Warunki skuteczności:***

- Żeby osiągnąć pełną skuteczność, zakres audytu powinien pod względem prawnym i technicznym obejmować przetwarzanie przez podmioty przetwarzające i podmioty podprzetwarzające podmiotu odbierającego danych osobowych przekazywanych do państwa trzeciego.
- Rejestry dostępu i inne podobne ślady powinny być zabezpieczone przed fałszowaniem, żeby audytorzy mogli znaleźć dowody ujawnienia. Rejestry dostępu i inne podobne ślady powinny również rozróżniać dostęp wynikający ze zwykłych czynności biznesowych i dostęp wynikający z nakazów lub żądań dostępu.

[80] Klauzula ta jest istotną gwarancją odpowiedniego stopnia ochrony przekazywanych danych osobowych i powinna być wymagana w większości przypadków.
[81] Zob. pkt 32.5 powyżej.
[82] Zob. np. Klauzula 5 lit. f) standardowych klauzul umownych między administratorami i podmiotami przetwarzającymi w decyzji 2010/87/UE, audyty mogłyby być również przeprowadzane na podstawie kodeksów postępowania lub poprzez certyfikację.

***

107. ***W przypadku gdy pierwotna ocena przepisów i praktyki państwa trzeciego wykazała stopień ochrony merytorycznie równoważny temu w UE dla danych przekazywanych przez podmiot przekazujący, podmiot przekazujący może wzmocnić obowiązek podmiotu odbierającego dane do niezwłocznego informowania podmiot przekazujący dane o niemożliwości wywiązania się z zobowiązań umownych i w efekcie zapewnienia wymaganego standardu „merytorycznie równoważnego stopnia ochrony danych.[83]"***

108. Brak takiej możliwości może wynikać ze zmian w przepisach lub praktykach państwa trzeciego[84]. Klauzule mogą przewidywać określone i sztywne terminy i procedury zapewniające szybkie zawieszenie przekazywania danych lub rozwiązanie umowy, a także zwrot lub usunięcie otrzymanych danych przez podmiot odbierający. Prowadzenie rejestru otrzymanych żądań, ich zakresu i skuteczności środków przyjętych w celu przeciwdziałania takim żądaniom powinno zapewnić podmiotowi przekazującemu wystarczające dowody, żeby wypełnić obowiązek zawieszenia lub zakończenia operacji przekazywania lub rozwiązania umowy.

109. ***Warunki skuteczności:***

- Powiadomienie musi mieć miejsce przed przyznaniem dostępu do danych. W przeciwnym razie, zanim podmiot przekazujący otrzyma powiadomienie, prawa jednostki mogły zostać już naruszone, jeśli żądanie opiera się na obowiązujących w takim państwie trzecim przepisach, które nie zapewniają stopnia ochrony wymaganego na podstawie prawa UE. Powiadomienie może służyć również do przeciwdziałania przyszłym naruszeniom i pozwolić podmiotowi przekazującemu zawiesić przekazywanie danych osobowych do państwa trzeciego lub rozwiązać umowę.
- Podmiot odbierający dane musi monitorować zmiany prawne i w polityce, które mogą doprowadzić do braku możliwości wywiązania się z obowiązków przez podmiot odbierający dane, i niezwłocznie powiadomić podmiot przekazujący dane o takich zmianach przed ich wejściem w życie (jeśli to możliwe), żeby pozwolić podmiotowi przekazującemu dane odzyskać dane od podmiotu odbierającego dane.
- Klauzule powinny przewidywać szybki mechanizm, za pomocą którego podmiot przekazujący dane zezwoli podmiotowi odbierającemu dane na niezwłoczne zabezpieczenie lub zwrócenie danych podmiotowi przekazującemu dane, a jeśli nie jest to możliwe – usunięcie lub bezpieczne zaszyfrowanie danych bez oczekiwania na instrukcje podmiotu przekazującego, jeśli zostanie osiągnięty określony próg uzgodniony między podmiotem przekazującym dane a podmiotem odbierającym dane. Podmiot odbierający dane powinien wdrożyć ten mechanizm od samego początku operacji przekazywania danych i regularnie przeprowadzać jego testy, żeby zapewnić, iż można go zastosować z krótkim wyprzedzeniem.

[83] Klauzula 5 lit. a) i lit. d) ppkt (i) standardowych klauzul umownych w decyzji 2010/87/UE.

[84] Zob. C-311/18 (Schrems II), pkt 139, gdzie Trybunał stwierdził, że „choć ta klauzula 5 lit. d) ppkt (i) pozwala podmiotowi odbierającemu dane osobowe w przypadku istnienia ustawodawstwa, które może on powołać na swoją obronę, takiego jak mający karny charakter zakaz mający na celu zachowanie tajemnicy dochodzenia policyjnego, na nieprzekazywanie mającemu siedzibę w Unii administratorowi danych prawnie wiążącego wniosku o ujawnienie danych osobowych ze strony organów ścigania, o tyle jest on jednak zobowiązany, zgodnie z zawartą w załączniku do decyzji w sprawie klauzul standardowych klauzulą 5 lit. a), do poinformowania tego administratora danych o swej niemożności spełnienia tego warunku zgodnie ze standardowymi klauzulami ochrony danych".

- Inne klauzule mogą pozwolić podmiotowi przekazującemu na monitorowanie przestrzegania tych obowiązków przez podmiot odbierający za pomocą audytów, inspekcji i innych środków weryfikacji, a także egzekwowanie ich za pomocą kar nałożonych na podmiot odbierający czy prawa podmiotu przekazującego do zawieszenia przekazywania lub rozwiązania umowy ze skutkiem natychmiastowym.

***

110. ***O ile jest to dozwolone na podstawie prawa krajowego państwa trzeciego, umowa może wzmacniać obowiązki w zakresie przejrzystości nałożone na podmiot odbierający poprzez wykorzystanie metody „Warrant Canary", zgodnie z którą podmiot odbierający przyjmuje na siebie zobowiązanie do regularnej wysyłki (np. przynajmniej co 24 godziny) kryptograficznie podpisanej wiadomości informującej podmiot przekazujący, że na dany dzień i daną godzinę nie otrzymał żadnego nakazu ujawnienia danych osobowych lub podobnego. Brak aktualizacji w tym zakresie może wskazywać podmiotowi przekazującemu, że podmiot odbierający mógł otrzymać nakaz.***

111. ***Warunki skuteczności:***

- Przepisy państwa trzeciego muszą pozwalać podmiotowi odbierającemu dane wysyłać takie bierne powiadomienia podmiotowi przekazującemu.
- Podmiot przekazujący musi automatycznie monitorować powiadomienia typu warrant canary.
- Podmiot odbierający musi zapewnić, że jego prywatny klucz wykorzystywany do podpisywania Warrant Canary przechowywany jest w bezpiecznym miejscu i że przepisy państwa trzeciego nie mogą zmusić podmiotu odbierającego do wysłania fałszywych powiadomień typu Warrant Canary. W tym celu użyteczne może być ustanowienie wymogu podpisu przez różne osoby lub wysyłki powiadomienia typu Warrant Canary przez osobę poza jurysdykcją państwa trzeciego.

Obowiązek podjęcia konkretnych działań

112. ***Podmiot odbierający może zobowiązać się do przeprowadzenia kontroli, zgodnie z prawem państwa docelowego, legalności nakazu ujawnienia danych, w szczególności w zakresie tego, czy znajduje się on w ramach właściwości żądającego organu publicznego, i zaskarżenia nakazu, jeśli po dogłębnej analizie dojdzie do wniosku, że zgodnie z prawem państwa docelowego są do tego podstawy. Zaskarżając nakaz, podmiot odbierający dane powinien złożyć wniosek o zastosowanie środków tymczasowych w celu wstrzymania skuteczności nakazu, dopóki sąd nie rozpatrzy sprawy co do istoty. Podmiot odbierający miałby zakaz ujawniania żądanych danych osobowych, dopóki nie będzie do tego zobowiązany na podstawie obowiązujących przepisów proceduralnych. Podmiot odbierający dane zobowiązałby się również do przekazania minimalnej dozwolonej ilości informacji w odpowiedzi na nakaz, zgodnie z zasadną interpretacją nakazu.***

113. ***Warunki skuteczności:***

- Porządek prawny państwa trzeciego musi oferować skuteczne środki prawne do zaskarżenia nakazów ujawnienia danych.
- Klauzula ta zawsze będzie zapewniać bardzo ograniczoną dodatkową ochronę, ponieważ nakaz ujawnienia danych może być zgodny z prawem w ramach porządku prawnego państwa

trzeciego, ale ten porządek prawny może nie spełniać standardów UE. Ten środek umowny będzie musiał być wsparty innymi środkami uzupełniającymi.
- Zaskarżenie nakazu musi mieć, na podstawie prawa państwa trzeciego, skutek zawieszający. W przeciwnym razie organy publiczne będą nadal mieć dostęp do danych osób fizycznych i wszelkie dalsze działania podjęte na rzecz osoby fizycznej będą mieć tylko ten skutek, że pozwolą jej dochodzić odszkodowania za negatywne konsekwencje wynikające z ujawnienia danych.
- Podmiot odbierający będzie musiał dokumentować i udowodnić podmiotowi przekazującemu, jakie działania podjął, dokładając wszelkich starań, w celu wywiązania się z tego zobowiązania.

***

114. ***W przypadku opisanym powyżej podmiot odbierający może zobowiązać się do powiadomienia żądającego organu publicznego o niezgodności nakazu z zabezpieczeniami zawartymi w narzędziu przekazywania z art. 46 RODO[85] i wynikającym z tego konflikcie obowiązków podmiotu odbierającego. Podmiot odbierający powiadomi jednocześnie i niezwłocznie podmiot przekazujący lub właściwy organ nadzorczy z EOG, jeśli jest to możliwe na podstawie porządku prawnego państwa trzeciego.***

115. ***Warunki skuteczności:***

- Takie informacje dotyczące ochrony zapewnianej przez prawo UE i konfliktu obowiązków powinny mieć jakiś skutek prawny na podstawie porządku prawnego państwa trzeciego, np. prowadzić do kontroli sądowej lub administracyjnej nakazu lub żądania dostępu, wymogu uzyskania nakazu sądowego lub tymczasowego zawieszenia wykonania nakazu w celu zapewnienia dodatkowej ochrony danych.
- System prawny państwa trzeciego nie może uniemożliwić podmiotowi odbierającemu powiadomienia podmiotu przekazującego lub chociaż właściwego organu nadzorczego w UE o nakazie lub żądaniu dostępu, jakie podmiot odbierający otrzymał.
- Podmiot odbierający będzie musiał dokumentować i udowodnić podmiotowi przekazującemu, jakie działania podjął, dokładając wszelkich starań, w celu wywiązania się z tego zobowiązania.

Przyznanie osobom, których dane dotyczą, dodatkowych uprawnień

116. ***Umowa może przewidywać, że dane osobowe przekazane w formie zwykłego tekstu w normalnym toku działalności (w tym w przypadku wsparcia) mogą być udostępnione wyłącznie za wyraźną lub dorozumianą zgodą podmiotu przekazującego lub osoby, której dane dotyczą.***

[85] Przykładowo standardowe klauzule umowne przewidują, że przetwarzanie i przekazywanie danych odbywało się i będzie się nadal odbywało zgodnie z „odpowiednimi przepisami właściwego prawa o ochronie danych". Prawo definiuje się jako „prawodawstwo chroniące podstawowe prawa i wolności osób fizycznych, a w szczególności ich prawo do prywatności w odniesieniu do przetwarzania danych osobowych, właściwe dla administratora danych w państwie członkowskim, w którym podmiot przekazujący dane prowadzi działalność gospodarczą". TSUE potwierdza, że przepisy RODO, odczytywane w świetle Karty praw podstawowych UE, stanowią część tego prawodawstwa, zob. wyrok TSUE w sprawie C-311/18 (Schrems II), pkt 138.

117. ***Warunki skuteczności:***

- Klauzula ta może być skuteczna w tych przypadkach, gdy podmioty odbierające dane otrzymują od organów publicznych żądania dobrowolnej współpracy, w przeciwieństwie do przypadków dostępu do danych przez organy publiczne bez wiedzy podmiotu odbierającego lub wbrew jego woli.
- W pewnych sytuacjach osoba, której dane dotyczą, może nie być w stanie przeciwstawić się dostępowi lub udzielić zgody, która spełniałaby wszystkie warunki określone prawem UE (dobrowolna, świadoma i jednoznaczna) (np. w przypadku pracowników)[86].
- Przepisy lub polityki krajowe nakładające na podmiot odbierający zakaz ujawniania nakazu dostępu mogą sprawić, że klauzula ta nie będzie skuteczna, chyba że zostanie ona wsparta metodami technicznymi wymagającymi działania ze strony podmiotu przekazującego lub osoby, której dane dotyczą, żeby można było uzyskać dostęp do danych w zwykłym tekście. Takie środki techniczne ograniczające dostęp mogą być przewidziane w szczególności wtedy, gdy dostęp przyznawany jest wyłącznie w konkretnych przypadkach wsparcia lub świadczenia usług, a same dane są przechowywane w EOG.

***

118. ***Umowa mogłaby nakładać na podmiot odbierający lub podmiot przekazujący obowiązek niezwłocznego powiadomienia osoby, której dane dotyczą, o żądaniu lub nakazie otrzymanym od organów publicznych państwa trzeciego lub o tym, że podmiot odbierający nie jest w stanie spełnić zobowiązań umownych w celu umożliwienia osobie, której dane dotyczą, uzyskania informacji lub złożenia skutecznego środka odwoławczego (np. poprzez wniesienie skargi do właściwego organu nadzorczego lub organu sądowego i wykazanie legitymacji czynnej w sądach państwa trzeciego).***

119. ***Warunki skuteczności:***

- Powiadomienie to może ostrzec osobę, której dane dotyczą, o potencjalnym dostępie do jej danych przez organy publiczne w państwie trzecim. Dzięki niemu osoba, której dane dotyczą, może uzyskać dodatkowe informacje od podmiotów przekazujących i wnieść skargę do właściwego organu nadzorczego. Klauzula ta może rozwiązać także niektóre problemy, jakie osoba fizyczna może mieć z wykazaniem legitymacji czynnej *(locus standi)* przed sądami państwa trzeciego w zakresie zaskarżenia dostępu organów publicznych do jej danych.
- Przepisy lub polityki krajowe mogą uniemożliwić powiadomienie osoby, której dane dotyczą. Podmiot przekazujący i podmiot odbierający mogą jednak zobowiązać się powiadomić osobę, której dane dotyczą, jak tylko ograniczenia ujawnienia danych zostaną zniesione, i dołożyć wszelkich starań, żeby uzyskać odstępstwo od zakazu ujawnienia. Jako niezbędne minimum podmiot przekazujący lub właściwy organ nadzorczy mogą powiadomić osobę, której dane dotyczą, o zawieszeniu lub zakończeniu przekazywania jej danych osobowych z tego względu, że podmiot odbierający nie jest w stanie wywiązać się ze swoich zobowiązań umownych w wyniku otrzymania żądania dostępu.

***

[86] Art. 4 ust. 11 RODO.

120. ***Umowa mogłaby nakładać na podmiot odbierający lub podmiot przekazujący obowiązek wsparcia osoby, której dane dotyczą, w wykonaniu przysługujących jej praw w ramach jurysdykcji państwa trzeciego za pomocą mechanizmów dochodzenia roszczeń ad hoc i doradztwa prawnego.***

121. ***Warunki skuteczności***

- Przepisy lub polityki krajowe mogą nałożyć warunki, które zniweczą skuteczność mechanizmów dochodzenia roszczeń *ad hoc*.
- Doradztwo prawne może być pomocne dla osoby, której dane dotyczą, biorąc zwłaszcza pod uwagę, jak skomplikowane i kosztowne może być zapoznanie się z systemem prawnym państwa trzeciego przez osobę, której dane dotyczą, i podjęcie działań prawnych z zagranicy, czasem w obcym języku. Klauzula ta zawsze będzie zapewniać bardzo ograniczoną dodatkową ochronę, ponieważ udzielanie wsparcia i świadczenie doradztwa prawnego na rzecz osób, których dane dotyczą, nie może samo w sobie zaradzić temu, że porządek prawny państwa trzeciego nie zapewnia stopnia ochrony merytorycznie równoważnego temu gwarantowanemu w UE. Ten środek umowny będzie musiał być wsparty innymi środkami uzupełniającymi.

Ten środek uzupełniający będzie skuteczny tylko wtedy, gdy przepisy państwa trzeciego przewidują możliwość dochodzenia roszczeń przed sądami krajowymi lub gdy istnieją mechanizmu dochodzenia roszczeń *ad hoc*. W każdym razie nie będzie to skuteczny środek uzupełniający chroniący przed narzędziami nadzoru, jeśli mechanizm dochodzenia roszczeń nie został przewidziany.

Środki organizacyjne

122. Dodatkowe środki organizacyjne mogą obejmować polityki wewnętrzne, metody organizacyjne i standardy, jakie administratorzy i podmioty przetwarzające stosują w ramach swojej organizacji i nakładają na podmioty odbierające dane w państwach trzecich. Mogą one przyczynić się do zapewnienia spójności ochrony danych osobowych w czasie całego cyklu przetwarzania. Środki organizacyjne mogą również podnosić świadomość podmiotów przekazujących o zagrożeniu i próbach uzyskania dostępu do danych w państwach trzecich oraz o możliwościach reakcji na takie okoliczności. Wybór i wdrożenie jednego z lub kilku tych środków nie zapewni w sposób pewny i systematyczny, że przeprowadzona operacja przekazywania spełni standard merytorycznie równoważnego stopnia ochrony wymaganego na podstawie prawa UE. W zależności od konkretnych okoliczności danej operacji przekazywania i przeprowadzonej oceny przepisów państwa trzeciego środki organizacyjne mogą być konieczne jako uzupełnienie środków prawnych lub technicznych w celu zapewnienia stopnia ochrony danych osobowych merytorycznie równoważnego temu gwarantowanemu w UE.

123. Ocenę najbardziej stosownych środków należy przeprowadzić osobno dla każdego przypadku, biorąc pod uwagę, że administratorzy i podmioty przetwarzające mają obowiązek przestrzegać zasady rozliczalności. EROD podaje poniżej listę przykładowych środków organizacyjnych, jakie podmioty przekazujące mogą wdrożyć, przy czym lista ta nie jest wyczerpująca i może nie obejmować wszystkich odpowiednich środków:

Polityki wewnętrzne w zakresie zarządzania przekazywaniem, zwłaszcza w grupach przedsiębiorstw

124. ***Przyjęcie adekwatnych polityk wewnętrznych przewidujących jasny podział obowiązków w zakresie przekazywania danych, kanały informacyjne i standardowe procedury operacyjne w przypadkach niejawnych lub oficjalnych żądań urzędów publicznych o dostęp do danych. W szczególności w przypadku przekazywania w ramach grupy przedsiębiorstw polityki te mogą przewidywać m.in.: powołanie specjalnego zespołu mającego siedzibę w EOG, złożonego z ekspertów z dziedziny IT, ochrony danych i prawa prywatności, który będzie obsługiwał żądania dotyczące danych osobowych przekazywanych z UE; powiadomienie kierownictwa prawnego i korporacyjnego wyższego szczebla i podmiotu przekazującego dane o otrzymaniu takich żądań; działania proceduralne zmierzające do zaskarżenia nieproporcjonalnych lub niezgodnych z prawem żądań oraz przekazanie osobom, których dane dotyczą, przejrzystych informacji.***

125. Opracowanie specjalnych procedur szkoleniowych dla pracowników odpowiedzialnych za obsługę żądań dostępu od organów publicznych, które należy okresowo aktualizować w celu uwzględnienia nowych zmian legislacyjnych i orzeczniczych w państwie trzecim i w EOG. Procedury szkoleniowe powinny uwzględniać wymogi prawa UE w zakresie dostępu organów publicznych do danych osobowych, w szczególności wynikające z art. 52 ust. 1 Karty praw podstawowych. Należy podnosić świadomość personelu w szczególności poprzez ocenę praktycznych przykładów żądań dostępu wystosowanych przez organy publiczne i poprzez zastosowanie do takich praktycznych przykładów standardu wynikającego z art. 52 ust. 1 Karty praw podstawowych. Szkolenia takie powinny brać pod uwagę szczególną sytuację podmiotu odbierającego dane, np. ustawodawstwo i uregulowania państwa trzeciego, którym podlega podmiot odbierający dane, i być w miarę możliwości opracowane we współpracy z podmiotem przekazującym dane.

126. ***Warunki skuteczności:***

- Polityki te mogą być przewidziane tylko w tych przypadkach, gdy żądanie dostępu wystosowane przez organy publiczne w państw trzecim jest zgodne z prawem UE[87]. Jeżeli jest niezgodne, polityki te nie będą wystarczające, żeby zapewnić równoważny stopień ochrony danych osobowych, w związku z czym - o czym była mowa powyżej - należy zaprzestać wszelkich operacji przekazywania lub wprowadzić odpowiednie środki uzupełniające w celu uniemożliwienia dostępu.

Środki związane z przejrzystością i rozliczalnością

127. ***Udokumentowanie i prowadzenie rejestru żądań dostępu otrzymanych od organów publicznych i udzielonych odpowiedzi, wraz z uzasadnieniem prawnym i zaangażowanymi podmiotami (np. jeżeli podmiot przekazujący został powiadomiony - również jego odpowiedzi i oceny zespołu ds. obsługi takich żądań itd.). Rejestry te należy udostępnić podmiotowi przekazującemu dane, który z kolei w razie potrzeby powinien przekazać je zainteresowanym osobom, których dane dotyczą.***

128. ***Warunki skuteczności:***

- Ustawodawstwo krajowe państwa trzeciego może uniemożliwić ujawnienie żądań lub istotnych informacji na ich temat, a tym samym sprawić, że środki te będą nieskuteczne.

[87] Zob. wyrok w sprawie C-362/14 („Schrems I"), pkt 94; C-311/18 (Schrems II), pkt 168, 174, 175 i 176.

Podmiot odbierający dane powinien powiadomić podmiot przekazujący o tym, że nie jest w stanie dostarczyć takich dokumentów i rejestrów, oferując tym samym podmiotowi przekazującemu możliwość zawieszenia przekazywania danych, jeżeli taka niezdolność prowadziłaby do obniżenia stopnia ochrony.

***

129. ***Regularna publikacja sprawozdań dotyczących przejrzystości lub streszczeń dotyczących żądań państwowych o dostęp do danych oraz rodzaju udzielonej odpowiedzi, w zakresie, w jakim publikacja jest dozwolona na mocy prawa lokalnego.***

130. ***Warunki skuteczności:***

- Przekazane informacje powinny być odpowiednie, jasne i możliwie jak najbardziej szczegółowe. Przepisy krajowe w państwie trzecim mogą uniemożliwiać ujawnienie szczegółowych informacji. W takim wypadku podmiot odbierający dane powinien dołożyć wszelkich starań, aby opublikować informacje statystyczne lub informacje zagregowane podobnego rodzaju.

Metody organizacyjne i środki minimalizacji danych

131. ***Uprzednie wymogi organizacyjne w ramach zasady rozliczalności, takie jak przyjęcie surowych i szczegółowych polityk i najlepszych praktyk w zakresie dostępu do danych i poufności, opartych na ścisłej zasadzie ograniczonego dostępu, monitorowanych za pomocą regularnych audytów i egzekwowanych za pomocą środków dyscyplinarnych, mogą być również użytecznymi środkami w kontekście przekazywania danych. W takich okolicznościach należy uwzględnić zasadę minimalizacji danych, aby ograniczyć narażenie danych osobowych na nieupoważniony dostęp. Przykładowo niekiedy może nie być potrzeby przekazania niektórych danych (np. w przypadku zdalnego dostępu do danych EOG, choćby w przypadkach wsparcia, gdy zamiast pełnego dostępu przyznaje się ograniczony dostęp; lub gdy świadczenie usługi wymaga jedynie przekazania ograniczonego zestawu danych, a nie całej bazy danych).***

132. ***Warunki skuteczności:***

- Należy prowadzić regularne audyty i podjąć zdecydowane środki dyscyplinarne w celu monitorowania i egzekwowania zgodności ze środkami minimalizacji danych również w kontekście przekazywania.
- Podmiot przekazujący dane powinien przed przekazaniem przeprowadzić ocenę posiadanych danych osobowych w celu zidentyfikowania tych zestawów danych, które nie są niezbędne dla celów przekazania, w związku z czym nie zostaną udostępnione podmiotowi odbierającemu dane.
- Środkom minimalizacji danych powinny towarzyszyć środki techniczne w celu zapewnienia, że dane nie są przedmiotem nieuprawnionego dostępu. Przykładowo, ustanowienie bezpiecznych mechanizmów obliczeń wielopodmiotowych i przekazanie zaszyfrowanych zestawów danych różnym zaufanym podmiotom może zapobiec w fazie projektowania jednostronnemu dostępowi prowadzącemu do ujawnienia danych umożliwiających identyfikację.

***

133. ***Opracowanie najlepszych praktyk w celu odpowiedniego i terminowego powiadomienia inspektora ochrony danych (jeżeli istnieje) oraz zespołów prawnych i zespołów ds. audytów wewnętrznych zapewnienia im dostępu do informacji dotyczących spraw związanych z międzynarodowym przekazywaniem danych osobowych.***

134. ***Warunki skuteczności:***

- Inspektor ochrony danych, jeżeli istnieje, oraz zespół prawny i zespół ds. audytów wewnętrznych otrzymają przed przekazaniem wszystkie stosowne informacje, a także będą konsultowani w sprawie niezbędności przekazania oraz ewentualnych dodatkowych zabezpieczeń.
- Stosowne informacje powinny obejmować m.in. ocenę niezbędności przekazania konkretnych danych osobowych, przegląd obowiązujących przepisów prawa państwa trzeciego oraz zabezpieczeń, do których wdrożenia podmiot odbierający się zobowiązał.

Przyjęcie norm i najlepszych praktyk

135. ***Przyjęcie surowszych polityk ochrony danych i prywatności danych, opartych na certyfikacji UE lub kodeksach postępowania bądź standardach międzynarodowych (np. normy ISO) i najlepszych praktykach (np. ENISA) z należytym uwzględnieniem aktualnego stanu wiedzy, zgodnie z ryzykiem związanym z kategoriami przetwarzanych danych i prawdopodobieństwem prób dostępu do nich ze strony organów publicznych.***

Inne

136. ***Przyjęcie i regularna weryfikacja wewnętrznych polityk dla celów oceny stosowności wdrożonych środków uzupełniających oraz w razie konieczności określenia i wdrożenia dodatkowych lub alternatywnych rozwiązań, aby zapewnić stopień ochrony przekazywanych danych osobowych równoważny temu gwarantowanemu w UE.***

***

137. ***Zobowiązanie podmiotu odbierającego dane do powstrzymania się od dalszego przekazania danych osobowych w tym samym lub innym państwie trzecim lub do zawieszenia ciągłego przekazywania, jeśli nie można zapewnić w państwie trzecim stopnia ochrony przekazywanych danych osobowych równoważnemu temu gwarantowanemu w UE.[88]***

[88] C-311/18 (Schrems II), pkt 135 i 137.

ZAŁĄCZNIK 3: MOŻLIWE ŹRÓDŁA INFORMACJI NA POTRZEBY OCENY PAŃSTWA TRZECIEGO

138. Podmiot odbierający dane powinien być w stanie podać stosowne źródła i informacje dotyczące państwa trzeciego, w którym prowadzi działalność, i przepisów, które znajdują do niego zastosowanie. Można także odwołać się do innych źródeł informacji, wymienionych na zasadzie przykładu poniżej:

- Orzecznictwo Trybunału Sprawiedliwości Unii Europejskiej (TSUE) i Europejskiego Trybunału Praw Człowieka (ETPC)[89], wymienione w zaleceniach w sprawie niezbędnych gwarancji europejskich;[90]
- Decyzje stwierdzające odpowiedni stopień ochrony w państwie docelowym, jeśli przekazywanie odbywa się na innej podstawie prawnej[91];
- Rezolucje i sprawozdania organizacji międzyrządowych, np. Rady Europy[92], innych instytucji regionalnych[93]; oraz organów i agencji ONZ (np. Rady Praw Człowieka ONZ[94], Komitetu Praw Człowieka[95]);
- Orzecznictwo krajowe i decyzje podjęte przez niezależne organy sądowe lub administracyjne właściwe ds. prywatności i ochrony danych w państwie trzecim;
- Raporty instytucji akademickich i organizacji społeczeństwa obywatelskiego (np. organizacji pozarządowych i organizacji branżowych).

[89] Zob. arkusz informacyjny dotyczący orzecznictwa ETPC w sprawie masowej inwigilacji: https://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf
[90] https://www.coe.int/en/web/data-protection/reports-studies-and-opinions
[91] C-311/18 (Schrems II), pkt 141; zob. decyzje stwierdzające odpowiedni stopień ochrony https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en
[92] https://www.coe.int/en/web/data-protection/reports-studies-and-opinions
[93] Zob. np. raporty krajowe Międzyamerykańskiej Komisji Praw Człowieka (IACHR), https://www.oas.org/en/iachr/reports/country.asp.
[94] Zob. https://www.ohchr.org/EN/HRBodies/UPR/Pages/Documentation.aspx
[95] Zob.: https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/TBSearch.aspx?Lang=en&TreatyID=8&DocTypeID=5

ZAŁĄCZNIK 1: DEFINICJE

- "Państwo trzecie" oznacza każde państwo, które nie jest państwem członkowskim EOG.
- "EOG" oznacza Europejski Obszar Gospodarczy i obejmuje państwa członkowskie Unii Europejskiej oraz Islandię, Norwegię i Liechtenstein. RODO dotyczy tych ostatnich na mocy Porozumienia o EOG, w szczególności jego załącznika XI and protokołu 37.
- "RODO" odnosi się do Rozporządzenia Parlamentu Europejskiego i Rady(UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).
- "Karta" odnosi się do Karty praw podstawowych Unii Europejskiej, OJ C 326, 26.10.2012 r., s. 391–407.
- "TSUE" lub "Trybunał" odnosi się do Trybunału Sprawiedliwości Unii Europejskiej. Stanowi on organ sądowy Unii Europejskiej i, we współpracy z sądami i trybunałami państw członkowskich, zapewnia jednolite stosowanie i interpretację prawa UE.
- "Podmiot przekazujący dane" oznacza administratora lub podmiot przekazujący w ramach EOG, który przekazuje dane osobowe do administratora lub podmiotu przetwarzającego w państwie trzecim.
- "Podmiot odbierający dane" oznacza administratora lub podmiot przekazujący w państwie trzecim, który otrzymuje lub uzyskuje dostęp do danych osobowych przekazywanych z EOG.
- "Narzędzie przekazywania z/na podstawie art. 46 RODO": odnosi się do odpowiednich zabezpieczeń na mocy artykułu 46 RODO, które podmioty przekazujące dane powinny wdrożyć przy przekazywaniu danych osobowych do państwa trzeciego, w razie braku decyzji stwierdzającej odpowiedni stopień ochrony na mocy artykułu 45 ust. 3 RODO. Artykuł 46 ust. 2 i ust. 3 RODO zawiera listę narzędzi przekazywania z artykułu 46 RODO, które administratorzy lub podmioty przetwarzające mogą wykorzystywać.
- "SCC" oznaczają standardowe klauzule ochrony danych (lub "standardowe klauzule umowne") przyjęte przez Komisję Europejską do celów przekazywania danych osobowych między administratorami lub podmiotami przetwarzającymi w EOG i administratorami lub podmiotami przetwarzającym spoza EOG. Standardowe klauzule umowne przyjęte przez Komisję Europejską stanowią narzędzie przekazywania na mocy RODO, zgodnie z artykułem 46 ust. 2 lit. c) i artykułem 46 ust. 5 RODO.

ANNEX 2: EXAMPLES OF SUPPLEMENTARY MEASURES

69. The following measures are examples of supplementary measures you could consider when you reach Step 4 "Adopt supplementary measures". This list is not exhaustive. Selecting and implementing one or several of these measures will not necessarily and systematically ensure that your transfer meets the essential equivalence standard that EU law requires. You should select those supplementary measures that can effectively guarantee this level of protection for your transfers.

70. Any supplementary measure may only be deemed effective in the meaning of the CJEU judgment "Schrems II" if and to the extent that it addresses the specific deficiencies identified in your assessment of the legal situation in the third country. If, ultimately, you cannot ensure an essentially equivalent level of protection, you must not transfer the personal data.

71. As a controller or processor, you may already be required to implement some of the measures described in this annex, even if your data importer is covered by an adequacy decision, just as you may be required to implement them when you process data within the EEA.[66]

Technical measures

72. This section describes in a non-exhaustive manner examples of technical measures, which may supplement safeguards found in Article 46 GDPR transfer tools to ensure compliance with the level of protection required under EU law in the context of a transfer of personal data to a third country. These measures will be especially needed where the law of that country imposes on the data importer obligations which are contrary to the safeguards of Article 46 GDPR transfer tools and are, in particular, capable of impinging on the contractual guarantee of an essentially equivalent level of protection against access by the public authorities of that third country to that data[67].

73. For further clarity, this section specifies first the technical measures that could potentially be effective in certain scenarios/use-cases to ensure an essentially equivalent level of protection. The section continues with some scenarios/use cases in which no technical measures could be found to ensure this level of protection.

Scenarios for which *effective* measures could be found

74. The measures listed below are intended to ensure that access to the transferred data by public authorities in third countries does not impinge on the effectiveness of the appropriate safeguards contained in the Article 46 GDPR transfer tools. These measures apply even if the public authorities' access complies with the law of the importer's country, where such access goes beyond what is necessary and proportionate in a democratic society[68]. These measures aim to preclude potentially infringing access by preventing the authorities from identifying the data subjects, inferring information about them, singling them out in another context, or associating the transferred data with other datasets they may possess that may contain, among other data, online identifiers provided by the devices, applications, tools and protocols used by data subjects in other contexts.

75. Public authorities in third countries may endeavour to access transferred data

    a) In transit by accessing the lines of communication used to convey the data to the recipient country. This access may be passive in which case the contents of the communication, possibly after a selection process, are simply copied. The access may, however, also be active in the sense that the public authorities interpose themselves into the communication process by not only reading the content, but also manipulating or suppressing parts of it.

    b) While in custody by an intended recipient of the data by either accessing the processing facilities themselves, or by requiring a recipient of the data to locate, and extract data of interest and turn it over to the authorities.

76. This section considers scenarios where measures are applied that are effective in both cases. Different supplementary measures may apply and be sufficient in the given circumstance of a concrete transfer if only one type of access is foreseen by the law of the recipient country. It is therefore necessary for the data exporter to carefully analyse, with the support of the data importer, the obligations laid upon the latter.

> As an example, US data importers that fall under 50 USC § 1881a (FISA 702) are under a direct obligation to grant access to or turn over imported personal data that are in their possession, custody or control. This may extend to any cryptographic keys necessary to render the data intelligible.

77. The scenarios describe specific circumstances, and measures taken. Any changes to the scenarios may give rise to different conclusions.

78. Controllers may have to apply some or all of the measures described here irrespective of the level of protection provided for by the laws applicable to the data importer because they are needed to comply with Articles 25 and 32 GDPR in the concrete circumstances of the transfer. In other words, exporters may be required to implement the measures described in this paper even if their data importers are covered by an adequacy decision, just as controllers and processors may be required to implement them when data is processed within the EEA.

Use Case 1: Data storage for backup and other purposes that do not require access to data in the clear

79. A data exporter uses a hosting service provider in a third country to store personal data, e.g., for backup purposes.

    If

    1. the personal data is processed using strong encryption before transmission,
    2. the encryption algorithm and its parameterization (e.g., key length, operating mode, if applicable) conform to the state-of-the-art and can be considered robust against cryptanalysis performed by the public authorities in the recipient country taking into account the resources and technical capabilities (e.g., computing power for brute-force attacks) available to them,
    3. the strength of the encryption takes into account the specific time period during which the confidentiality of the encrypted personal data must be preserved,

[66] Article 5.2 GDPR, Article 32 GDPR.
[67] C-311/18 (Schrems II), paragraph 135.
[68] See Articles 47 and 52 of the EU Charter of Fundamental Rights, Article 23.1 GDPR, and EDPB Recommendations on the European Essential Guarantees for Surveillance Measures.

4. the encryption algorithm is flawlessly implemented by properly maintained software the conformity of which to the specification of the algorithm chosen has been verified, e.g., by certification,
5. the keys are reliably managed (generated, administered, stored, if relevant, linked to the identity of an intended recipient, and revoked), and
6. the keys are retained solely under the control of the data exporter, or other entities entrusted with this task which reside in the EEA or a third country, territory or one or more specified sectors within a third country, or at an international organisation for which the Commission has established in accordance with Article 45 GDPR that an adequate level of protection is ensured,

then the EDPB considers that the encryption performed provides an effective supplementary measure.

Use Case 2: Transfer of pseudonymised Data

80. A data exporter first pseudonymises data it holds, and then transfers it to a third country for analysis, e.g., for purposes of research.

If

1. a data exporter transfers personal data processed in such a manner that the personal data can no longer be attributed to a specific data subject, nor be used to single out the data subject in a larger group, without the use of additional information[69],
2. that additional information is held exclusively by the data exporter and kept separately in a Member State or in a third country, territory or one or more specified sectors within a third country, or at an international organisation for which the Commission has established in accordance with Article 45 GDPR that an adequate level of protection is ensured,
3. disclosure or unauthorised use of that additional information is prevented by appropriate technical and organisational safeguards, it is ensured that the data exporter retains sole control of the algorithm or repository that enables re-identification using the additional information, and
4. the controller has established by means of a thorough analysis of the data in question taking into account any information that the public authorities of the recipient country may possess that the pseudonymised personal data cannot be attributed to an identified or identifiable natural person even if cross-referenced with such information,

then the EDPB considers that the pseudonymisation performed provides an effective supplementary measure.

81. Note that in many situations, factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of a natural person, their physical location or their interaction with an internet

[69] In line with Article 4(5) GDPR: "'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;".

based service at specific points in time[70] may allow the identification of that person even if their name, address or other plain identifiers are omitted.

82. This is particularly true whenever the data concern the use of information services (time of access, sequence of features accessed, characterisitics of the device used etc.). These services might well be, as for the importer of personal data, under the obligation to grant access to the same public authorities in their jurisdiction, which will then likely possess data about the use of those information services by the person(s) they target.

83. Moreover, given the use of some information services is public by nature, or their exploitability by parties with substantial resources, controllers will have to take extra care considering that public authorities in their jurisdiction likely possess data about the use of information services by a person they target.

Use Case 3: Encrypted data merely transiting third countries

84. A data exporter wishes to transfer data to a destination recognised as offering adequate protection in accordance with Article 45 GDPR. The data is routed via a third country.

If

1. a data exporter transfers personal data to a data importer in a jurisdiction ensuring adequate protection, the data is transported over the internet, and the data may be geographically routed through a third country not providing an essentially equivalent level of protection,
2. transport encryption is used for which it is ensured that the encryption protocols employed are state-of-the-art and provide effective protection against active and passive attacks with resources known to be available to the public authorities of the third country,
3. decryption is only possible outside the third country in question,
4. the parties involved in the communication agree on a trustworthy public-key certification authority or infrastructure,
5. specific protective and state-of-the-art measures are used against active and passive attacks on transport-encrypted,
6. in case the transport encryption does not provide appropriate security by itself due to experience with vulnerabilities of the infrastructure or the software used, personal data is also encrypted end-to-end on the application layer using state-of-the-art encryption methods,
7. the encryption algorithm and its parameterization (e.g., key length, operating mode, if applicable) conform to the state-of-the-art and can be considered robust against cryptanalysis performed by the public authorities in the transiting country taking into account the resources and technical capabilities (e.g., computing power for brute-force attacks) available to them,
8. the strength of the encryption takes into account the specific time period during which the confidentiality of the encrypted personal data must be preserved,
9. the encryption algorithm is flawlessly implemented by properly maintained software the conformity of which to the specification of the algorithm chosen has been verified, e.g., by certification,

[70] Art. 4(1) GDPR: "' personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;".

10. the existence of backdoors (in hardware or software) has been ruled out,
11. the keys are reliably managed (generated, administered, stored, if relevant, linked to the identity of the intended recipient, and revoked), by the exporter or by an entity trusted by the exporter under a jurisdiction offering an essentially equivalent level of protection,

then the EDPB considers that transport encryption, if needed in combination with end-to-end content encryption, provides an effective supplementary measure.

Use Case 4: Protected recipient

85. A data exporter transfers personal data to a data importer in a third country specifically protected by that country's law, e.g., for the purpose to jointly provide medical treatment for a patient, or legal services to a client.

If

1. the law of a third country exempts a resident data importer from potentially infringing access to data held by that recipient for the given purpose, e.g. by virtue of a duty to professional secrecy applying to the data importer,
2. that exemption extends to all information in the possession of the data importer that may be used to circumvent the protection of privileged information (cryptographic keys, passwords, other credentials, etc.),
3. the data importer does not employ the services of a processor in a way that allows the public authorities to access the data while held by the processor, nor does the data importer forward the data to another entity that is not protected, on the basis of Article 46 GDPR transfer tools,
4. the personal data is encrypted before it is transmitted with a method conforming to the state of the art guaranteeing that decryption will not be possible without knowledge of the decryption key (end-to-end encryption) for the whole length of time the data needs to be protected,
5. the decryption key is in the sole custody of the protected data importer, and appropriately secured against unauthorised use or disclosure by technical and organisational measures conforming to the state of the art, and
6. the data exporter has reliably established that the encryption key it intends to use corresponds to the decryption key held by the recipient,

then the EDPB considers that the transport encryption performed provides an effective supplementary measure.

Use Case 5: Split or multi-party processing

86. The data exporter wishes personal data to be processed jointly by two or more independent processors located in different jurisdictions without disclosing the content of the data to them. Prior to transmission, it splits the data in such a way that no part an individual processor receives suffices to reconstruct the personal data in whole or in part. The data exporter receives the result of the processing from each of the processors independently, and merges the pieces received to arrive at the final result which may constitute personal or aggregated data.

If

1. a data exporter processes personal data in such a manner that it is split into two or more parts each of which can no longer be interpreted or attributed to a specific data subject without the use of additional information,
2. each of the pieces is transferred to a separate processor located in a different jurisdiction,
3. the processors optionally process the data jointly, e.g. using secure multi-party computation, in a way that no information is revealed to any of them that they do not possess prior to the computation,
4. the algorithm used for the shared computation is secure against active adversaries,
5. there is no evidence of collaboration between the public authorities located in the respective jurisdictions where each of the processors are located, which would allow them access to all sets of personal data held by the processors and enable them to reconstitute and exploit the content of the personal data in a clear form in circumstances where such exploitation would not respect the essence of the fundamental rights and freedoms of the data subjects. Similarly, public authorities of either country should not have the authority to access personal data held by processors in all jurisdictions concerned.
6. the controller has established by means of a thorough analysis of the data in question, taking into account any information that the public authorities of the recipient countries may possess, that the pieces of personal data it transmits to the processors cannot be attributed to an identified or identifiable natural person even if cross-referenced with such information,

then the EDPB considers that the split processing performed provides an effective supplementary measure.

Scenarios in which *no effective* measures could be found

87. The measures described below under certain scenarios would not be effective in ensuring an essentially equivalent level of protection for the data transferred to the third country. Therefore, they would not qualify as supplementary measures.

Use Case 6: Transfer to cloud services providers or other processors which require access to data in the clear

88. A data exporter uses a cloud service provider or other processor to have personal data processed according to its instructions in a third country.

If

1. a controller transfers data to a cloud service provider or other processor,
2. the cloud service provider or other processor needs access to the data in the clear in order to execute the task assigned, and
3. the power granted to public authorities of the recipient country to access the transferred data goes beyond what is necessary and proportionate in a democratic society,[71]

[71] See Articles 47 and 52 of the EU Charter of Fundamental Rights, Article 23.1 GDPR, and EDPB Recommendations on the European Essential Guarantees for Surveillance Measures.

then the EDPB is, considering the current state of the art, incapable of envisioning an effective technical measure to prevent that access from infringing on data subject rights. The EDPB does not rule out that further technological development may offer measures that achieve the intended business purposes, without requiring access in the clear.

89. In the given scenarios, where unencrypted personal data is technically necessary for the provision of the service by the processor, transport encryption and data-at-rest encryption even taken together, do not constitute a supplementary measure that ensures an essentially equivalent level of protection if the data importer is in possession of the cryptographic keys.

Use Case 7: Remote access to data for business purposes

90. A data exporter makes personal data available to entities in a third country to be used for shared business purposes. A typical constellation may consist of a controller or processor established on the territory of a Member State transferring personal data to a controller or processor in a third country belonging to the same group of undertakings, or group of enterprises engaged in a joint economic activity. The data importer may, for example, use the data it receives to provide personnel services for the data exporter for which it needs human resources data, or to communicate with customers of the data exporter who live in the European Union by phone or email.

    If

    1. a data exporter transfers personal data to a data importer in a third country by making it available in a commonly used information system in a way that allows the importer direct access of data of its own choice, or by transferring it directly, individually or in bulk, through use of a communication service,
    2. the importer uses the data in the clear for its own purposes,
    3. the power granted to public authorities of the recipient country to access the transferred data goes beyond what is necessary and proportionate in a democratic society,

    then the EDPB is incapable of envisioning an effective technical measure to prevent that access from infringing on data subject rights.

91. In the given scenarios, where unencrypted personal data is technically necessary for the provision of the service by the processor, transport encryption and data-at-rest encryption even taken together, do not constitute a supplementary measure that ensures an essentially equivalent level of protection if the data importer is in possession of the cryptographic keys.

Additional contractual measures

92. These measures will generally consist of unilateral, bilateral or multilateral[72] contractual commitments.[73] If an Article 46 GDPR transfer tool is used, it will in most cases already contain a number of (mostly contractual) commitments by the data exporter and the data importer aimed at serving as safeguards for the personal data.[74]

93. In some situations, these measures may complement and reinforce the safeguards the transfer tool and relevant legislation of the third country may provide, when, taking into account the circumstances of the transfer, these do not meet all the conditions required to ensure a level of protection essentially equivalent to that guaranteed within the EU. Provided the nature of contractual measures, generally not capable of binding the authorities of that third country, when they are not party to the contract[75], these measures should be combined with other technical and organisational measures to provide the level of data protection required. Selecting and implementing one or several of these measures will not necessarily and systematically ensure that your transfer meets the essential equivalence standard that EU law requires.

94. Depending on what contractual measures are already included in the Article 46 GDPR transfer tool that is relied on, additional contractual measures may also be helpful to allow EEA-based data exporters to become aware of new developments affecting the protection of the data transferred to third countries.

95. As said, contractual measures will not be able to rule out the application of the legislation of a third country which does not meet the EDPB European Essential Guarantees standard in those cases in which the legislation obliges importers to comply with the orders to disclose data they receive from public authorities.[76]

96. Some examples of these potential contractual measures are listed below and classified in accordance with their nature:

Providing for the contractual obligation to use specific technical measures

97. Depending on the specific circumstances of the transfers, the contract may need to provide that for transfers to take place, specific technical measures would have to be put in place (see supra the technical measures suggested).

98. Conditions for effectiveness:

[72] E.g. within BCRs which should in any case regulate some of the measures listed below.
[73] They will have a private nature and not be considered as international agreements under public international law. Accordingly, they will normally fail to bind the third country's public authority as non-parties to the contract when concluded with private bodies in third countries, as the Court underlined in its judgment C-311/18 (Schrems II), paragraph 125.
[74] See judgment C-311/18 (Schrems II), paragraph 137 where the Court as a result recognised that the SCC contain *« effective mechanisms that make it possible, in practice, to ensure compliance with the level of protection required by EU law and that transfers of personal data pursuant to the clauses of such a decision are suspended or prohibited in the event of the breach of such clauses or it being impossible to honour them »* see also paragraph 148).
[75] C-311/18 (Schrems II), paragraph 125.
[76] CJEU judgment C-311/18 (Schrems II), paragraph 132.

- This clause could be effective in those situations where the need for technical measures has been identified by the exporter. It would then have to be provided in a legal form to ensure that the importer also commits to put in place the necessary technical measures if need be.

Transparency obligations:

99. ***The exporter could add annexes to the contract with information that the importer would provide, based on its best efforts, on the access to data by public authorities, including in the field of intelligence provided the legislation complies with the EDPB European Essential Guarantees, in the destination country. This might help the data exporter to meet its obligation to document its assessment of the level of protection in the third country.***

100. The importer could be for instance required to:

(1) enumerate the laws and regulations in the destination country applicable to the importer or its (sub) processors that would permit access by public authorities to the personal data that are subject to the transfer, in particular in the areas of intelligence, law enforcement, administrative and regulatory supervision applicable to the transferred data;
(2) in the absence of laws governing the public authorities' access to data provide information and statistics based on the importer's experience or reports from various sources (e.g. partners, open sources, national case law and decisions from oversight bodies) on access by public authorities to personal data in situations of the kind of the data transfer at hand (i.e. in the specific regulatory area; regarding the type of entities to which the data importer belongs;...)
(3) indicate which measures are taken to prevent the access to transferred data (if any);
(4) provide sufficiently detailed information on all requests of access to personal data by public authorities which the importer has received over a specified period of time,[77] in particular in the areas mentioned under (1) above and comprising information about the requests received, the data requested, the requesting body and the legal basis for disclosure and to what extent the importer has disclosed the data request;[78]
(5) specify whether and to what extent the importer is legally prohibited to provide the information mentioned under (1) – (5) above.

101. This information could be provided by way of structured questionnaires that the importer would fill in and sign and compounded by the importer's contractual obligation to declare within a set period of time any potential change to this information, as is current practice for due diligence processes.

102. ***Conditions for effectiveness:***

- The importer must be able to provide the exporter with these types of information to the best of its knowledge and after having used its best efforts to obtain it.[79]

[77] The length of period should depend on the risk for the rights and freedoms of the data subjects whose data are subject to the transfer at stake – e.g. the last year before closure of the data export instrument with the data exporter
[78] Complying with this duty does not as such amount to providing for an appropriate level of protection. At the same time any inappropriate disclosure that has actually happened leads to the necessity of implementing supplementary measures.
[79] See paragraph 32.5 above.

- This obligation imposed on the importer is a means to ensure that the exporter becomes and remains aware of the risks attached to the transfer of data to a third country. It will thus enable the exporter to desist from concluding the contract, or if the information changes following its conclusion, to fulfil its obligation to suspend the transfer and/or terminate the contract if the law of the third country, the safeguards contained in the Article 46 GDPR transfer tool used and any additional safeguards it may have adopted can no longer ensure a level of protection essentially equivalent to that in the EU. This obligation can however neither justify the importer's disclosure of personal data nor give rise to the expectation that there will be no further access requests.

***

103. ***The exporter could also add clauses whereby the importer certifies that (1) it has not purposefully created back doors or similar programming that could be used to access the system and/or personal data (2) it has not purposefully created or changed its business processes in a manner that facilitates access to personal data or systems, and (3) that national law or government policy does not require the importer to create or maintain back doors or to facilitate access to personal data or systems or for the importer to be in possession or to hand over the encryption key.[80]***

104. ***Conditions for effectiveness:***

- The existence of legislation or government policies preventing importers from disclosing this information may render this clause ineffective. The importer will thus not be able to enter into the contract or will need to notify to the exporter of its inability to continue complying with its contractual commitments.[81]
- The contract must include penalties and/or the exporter's ability to terminate the contract on short notice in those cases in which the importer does not reveal the existence of a back door or similar programming or manipulated business processes or any requirement to implement any of these or fails to promptly inform the exporter once their existence comes to its knowledge.

***

105. ***The exporter could reinforce its power to conduct audits[82] or inspections of the data processing facilities of the importer, on-site and/or remotely, to verify if data was disclosed to public authorities and under which conditions (access not beyond what is necessary and proportionate in a democratic society), for instance by providing for a short notice and mechanisms ensuring the rapid intervention of inspection bodies and reinforcing the autonomy of the exporter in selecting the inspection bodies.***

106. ***Conditions for effectiveness:***

- The scope of the audit should legally and technically cover any processing by the importer's processors or sub-processors of the personal data transmitted in the third country to be fully effective.

[80] This clause is important to guarantee an adequate level of protection of the personal data transferred and should usually be required.
[81] See paragraph 32.5 above.
[82] See for instance Clause 5.f of SCCs between controllers and processors Decision 2010/87/EU, the audits could also be provided within a code of conduct or through certification.

- Access logs and other similar trails should be tamper proof so that the auditors can find evidence of disclosure. Access logs and other similar trails should also distinguish between accesses due to regular business operations and accesses due to orders or requests for access.

***

107. Where the law and practice of the third country of the importer was initially assessed and deemed to provide an essentially equivalent level of protection as provided in the EU for data transferred by the exporter, the exporter could still strengthen the obligation of the data importer to inform promptly the data exporter of its inability to comply with the contractual commitments and as a result with the required standard of "essentially equivalent level of data protection".[83]

108. This inability to comply may result from changes in the third country's legislation or practice.[84] The clauses could set specific and strict time limits and procedures for the swift suspension of the transfer of data and/or the termination of the contract and the importer's return or deletion of the data received. Keeping track of the requests received, their scope, and the effectiveness of the measures adopted to counter them, should provide the exporter with sufficient indications to exercise its duty to suspend or end the transfer and/or terminate the contract.

109. Conditions for effectiveness:

- The notification needs to take place before access is granted to the data. Otherwise, by the time the exporter receives the notification, the rights of the individual may have already been violated if the request is based on laws of that third country that exceed what the level of data protection afforded under EU law permits. The notification may still serve to prevent future violations and to allow the exporter to fulfil its duty to suspend the transfer of personal data to the third country and/or terminate the contract.
- The data importer must monitor any legal or policy developments that might lead to its inability to comply with its obligations, and promptly inform the data exporter of any such changes and developments, and if possible ahead of their implementation to enable the data exporter to recover the data from the data importer.
- The clauses should provide for a quick mechanism whereby the data exporter authorises the data importer to promptly secure or return the data to the data exporter, or if this is not feasible, delete or securely encrypt the data without necessarily waiting for the exporter's instructions, if a specific threshold to be agreed between the data exporter and the data importer is met. The importer should implement this mechanism from the beginning of the data transfer and test it regularly to ensure that it can be applied on short notice.
- Other clauses could enable the exporter to monitor the importer's compliance with these obligations via audits, inspections and other verification measures and to enforce them with penalties on the importer and/or the exporter's capacity to suspend the transfer and/or terminate immediately the contract.

[83] Clause 5.a and d.i of SCCs Decision 2010/87/EU.

[84] See C-311/18 (Schrems II), paragraph 139 in which the Court asserts that *"although Clause 5(d)(i) allows a recipient of personal data not to notify a controller established in the European Union of a legally binding request for disclosure of the personal data by a law enforcement authority, in the event of legislation prohibiting that recipient from doing so, such as a prohibition under criminal law the aim of which is to preserve the confidentiality of a law enforcement investigation, the recipient is nevertheless required, pursuant to Clause 5(a) in the annex to the SCC Decision, to inform the controller of his or her inability to comply with the standard data protection clauses."*

***

110. Insofar as allowed by national law in the third country, the contract could reinforce the transparency obligations of the importer by providing for a "Warrant Canary" method, whereby the importer commits to regularly publish (e.g. at least every 24 hours) a cryptographically signed message informing the exporter that as of a certain date and time it has received no order to disclose personal data or the like. The absence of an update of this notification will indicate to the exporter that the importer may have received an order.

111. Conditions for effectiveness:

- The regulations of the third country must permit the data importer to issue this form of passive notification to the exporter.
- The data exporter must automatically monitor the warrant canary notifications.
- The data importer must ensure that its private key for signing the Warrant Canary is kept safe and that it cannot be forced to issue false Warrant Canaries by the regulations of the third country. To this end, it might be of use if several signatures by different persons are needed and/or the Warrant Canary is issued by a person outside the third country's jurisdiction.

Obligations to take specific actions

112. The importer could commit to reviewing, under the law of the country of destination, the legality of any order to disclose data, notably whether it remains within the powers granted to the requesting public authority, and to challenge the order if, after a careful assessment, it concludes that there are grounds under the law of the country of destination to do so. When challenging an order, the data importer should seek interim measures to suspend the effects of the order until the court has decided on the merits. The importer would have the obligation not to disclose the personal data requested until required to do so under the applicable procedural rules. The data importer would also commit to providing the minimum amount of information permissible when responding to the order, based on a reasonable interpretation of the order.

113. Conditions for effectiveness:

- The legal order of the third country must offer effective legal avenues to challenge orders to disclose data.
- This clause will always offer a very limited additional protection as an order to disclose data may be lawful under the legal order of the third country, but this legal order may not meet EU standards. This contractual measure will necessarily need to be complementary to other supplementary measures.
- The challenges to the orders must have a suspensive effect under the law of the third country. Otherwise, public authorities would still have access to the individuals' data and any ensuing action in favor of the individual would have the limited effect of allowing him/her to claim damages for negative consequences resulting from the data disclosure.
- The importer will need to be able to document and demonstrate to the exporter the actions it has taken, exercising its best efforts, to fulfill this commitment.

***

114. In the same situation as described above, the the importer could commit to inform the requesting public authority of the incompatibility of the order with the safeguards contained in the Article 46 GDPR transfer tool[85] and the resulting conflict of obligations for the importer. The importer would notify simultaneously and as soon as possible the exporter and/or the competent supervisory authority from the EEA, insofar as possible under the third country legal order.

115. Conditions for effectiveness:

- Such information on the protection conferred by EU law and the conflict of obligations should have some legal effect in the legal order of the third country, such as a judicial or administrative review of the order or request for access, the requirement of a judicial warrant, and/or a temporary suspension of the order to add some protection to the data.
- The legal system of the country must not prevent the importer from notifying the exporter or at least the competent supervisory authority from the EEA of the order or request for access received.
- The importer will need to be able to document and demonstrate to the exporter the actions it has taken, exercising its best efforts, to fulfill this commitment.

Empowering data subjects to exercise their rights

116. The contract could provide that personal data transmitted in plain text in the normal course of business (including in support cases) may only be accessed with the express or implied consent of the exporter and/or the data subject.

117. Conditions for effectiveness:

- This clause could be effective in those situations in which importers receive requests from public authorities to cooperate on a voluntary basis, as opposed to e.g. data access by public authorities that occurs without the data importer's knowledge or against its will.
- In some situations the data subject may not be in a position to oppose the access or to give a consent that meets all the conditions set out under EU law (freely given, specific, informed, and unambiguous) (e.g in the case of employees)[86].
- National regulations or policies compelling the importer not to disclose the order for access may render this clause ineffective, unless it can be backed with technical methods requiring the exporter's or the data subject's intervention for the data in plant text to be accessible. Such technical measures to restrict access may be envisaged in particular if access is only granted in specific support or service cases, but the data itself is stored in the EEA.

[85] For instance, the SCCs provide that the processing of data, including the transfer thereof, has been and will continue to be carried out in accordance with *"the applicable data protection law"*. This law is defined as *"the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established"*. The CJEU confirms that the provisions of the GDPR, read in light of the EU Charter of Fundamental rights, form part of that legislation, see CJEU C-311/18 (Schrems II), paragraph 138.
[86] Article 4(11) GDPR.

***

118. The contract could oblige the importer and/or the exporter to notify promptly the data subject of the request or order received from the public authorities of the third country, or of the importer's inability to comply with the contractual commitments, to enable the data subject to seek information and an effective redress (e.g. by lodging a claim with his/her competent supervisory authority and/or judicial authority and demonstrate his/her standing in the courts of the third country).

119. Conditions for effectiveness:

- This notification could alert the data subject to potential accesses by public authorities in third countries to his/her data. It could thus enable the data subject to seek additional information with the exporters and to lodge a claim with his/her competent supervisory authority. This clause could also address some of the difficulties an individual may face in demonstrating his/her standing *(locus standi)* before third country courts to challenge the public authorities' access to his/her data.
- National regulations and policies may prevent this notification to the data subject. The exporter and importer could nonetheless commit to informing the data subject as soon as the restrictions on the disclosure of data are lifted and to make its best efforts to obtain the waiver of the prohibition to disclose. At a minimum, the exporter or the competent supervisory authority could notify the data subject of the suspension or termination of the transfer of his/her personal data due to the importer's inability to comply with its contractual commitments as a result of its receipt of a request for access.

***

120. The contract could commit the exporter and importer to assist the data subject in exercising his/her rights in the third country jurisdiction through ad hoc redress mechanisms and legal counselling.

121. Conditions for effectiveness

- National regulations and policies may impose conditions that may undermine the effectiveness of the ad hoc redress mechanisms provided for.
- Legal counselling could be helpful for the data subject, especially considering how complex and costly it can be for a data subject to understand a third country's legal system and to exercise legal actions from abroad, potentially in a foreign language. However, this clause will always offer a limited additional protection, as providing assistance and legal counselling to data subjects cannot in itself remedy a third country's legal order failure to provide for a level of protection essentially equivalent to that guaranteed within the EU. This contractual measure will necessarily need to be complementary to other supplementary measures.

This supplementary measure would only be effective provided that the law of the third country provides for redress before its national courts or that an ad hoc redress mechanism exist. In any case, this would however not be an efficient supplementary measure against surveillance measures if no redress mechanism exists.

Organisational measures

122. Additional organisational measures may consist of internal policies, organisational methods, and standards controllers and processors could apply to themselves and impose on the importers of data in third countries. They may contribute to ensuring consistency in the protection of personal data during the full cycle of the processing. Organisational measures may also improve the exporters' awareness of risk of and attempts to gain access to the data in third countries, and their capacity to react to them. Selecting and implementing one or several of these measures will not necessarily and systematically ensure that your transfer meets the essential equivalence standard that EU law requires. Depending on the specific circumstances of the transfer and the assessment performed on the legislation of the third country, organisational measures are needed to complement contractual and/or technical measures, in order to ensure a level of protection of the personal data essentially equivalent to that guaranteed within the EU.

123. The assessment of the most suitable measures has to be done on a case by cases basis keeping in mind the need for controllers and processors to respect the accountability principle. Below, the EDPB lists some examples of organisational measures that exporters can implement, albeit the list is not exhaustive and other measures may also be appropriate :

Internal policies for governance of transfers especially with groups of enterprises

124. Adoption of adequate internal policies with clear allocation of responsibilities for data transfers, reporting channels and standard operating procedures for cases of covert or official requests from public authorities to access the data. Especially in case of transfers among groups of enterprises, these policies may include, among others, the appointment of a specific team, which should be based within the EEA, composed by experts on IT, data protection and privacy laws, to deal with requests that involve personal data transferred from the EU; the notification to the senior legal and corporate management and to the data exporter upon receipt of such requests; the procedural steps to challenge disproportionate or unlawful requests and the provision of transparent information to data subjects.

125. Development of specific training procedures for personnel in charge of managing requests for access to personal data from public authorities, which should be periodically updated to reflect new legislative and jurisprudential developments in the third country and in the EEA. The training procedures should include the requirements of EU law as to access by public authorities to personal data, in particular as following from Article 52 (1) of the Charter of Fundamental Rights. Awareness of personnel should be raised in particular by means of assessment of practical examples of public authorities' data access requests and by applying the standard following from Article 52(1) of the Charter of Fundamental Rights to such practical examples. Such training should take into account the particular situation of the data importer, e.g. legislation and regulations of the third country to which the data importer is subject to, and should be developed where possible in cooperation with the data exporter.

126. Conditions for effectiveness:

- These policies may only be envisaged for those cases where the request from public authorities in the third country is compatible with EU law.[87] When the request is incompatible, these policies would not suffice to ensure an equivalent level of protection of the personal data and, as said above, transfers must be stopped or appropriate supplementary measures to avoid the access must be put in place.

[87] See Case C-362/14 (« Schrems I »), par. 94; C-311/18 (Schrems II), paragraphs 168, 174, 175 and 176.

Transparency and accountability measures

127. Document and record the requests for access received from public authorities and the response provided, alongside the legal reasoning and the actors involved (e.g. if the exporter has been notified and its reply, the assessment of the team in charge of dealing with such requests, etc.). These records should be made available to the data exporter, who should in turn provide them to the data subjects concerned where required.

128. Conditions for effectiveness:

- National legislation in the third country may prevent disclosure of the requests or substantial information thereof and therefore render this practice ineffective. The data importer should inform the exporter of its inability to provide such documents and records, thus offering the exporter the option to suspend the transfers if such inability would lead to a decrease of the level of protection.

***

129. Regular publication of transparency reports or summaries regarding governmental requests for access to data and the kind of reply provided, insofar publication is allowed by local law.

130. Conditions for effectiveness:

- The information provided should be relevant, clear and as detailed as possible. National legislation in the third country may prevent disclosure of detailed information. In those cases, the data importer should employ its best efforts to publish statistical information or similar type of aggregated information.

Organisation methods and data minimisation measures

131. Already existing organisational requirements under the accountability principle, such as the adoption of strict and granular data access and confidentiality policies and best practices, based on a strict need-to-know principle, monitored with regular audits and enforced through disciplinary measures may also be useful measures in a transfer context. Data minimisation should be considered in this regard, in order to limit the exposure of personal data to unauthorised access. For example, in some cases it might not be necessary to transfer certain data (e.g. in case of remote access to EEA data, such as in support cases, when restricted access is granted instead of full access; or when the provision of a service only requires the transfer of a limited set of data, and not an entire database).

132. Conditions for effectiveness:

- Regular audits and strong disciplinary measures should be in place in order to monitor and enforce compliance with the data minimisation measures also in the transfer context.

- The data exporter shall perform an assessment of the personal data in its possession before the transfer takes place, in order to identify those sets of data that are not necessary for the purposes of the transfer and, therefore, won't be shared with the data importer.
- Data minimisation measures should be accompanied with technical measures as to ensure that data are not subject to unauthorised access. For example, the implementation of secure multiparty computation mechanisms and the spread of encrypted datasets among different trusted entities can prevent by design that any unilateral access lead to the disclosure of identifiable data.

***

133. ***Development of best practices to appropriately and timely involve and provide access to information to the data protection officer, if existent, and to the legal and internal auditing services on matters related to international transfers of personal data transfers.***

134. ***Conditions for effectiveness:***

- The data protection officer, if existent, and the legal and internal auditing team shall be provided with all the relevant information prior to the transfer, and shall be consulted on the necessity of the transfer and the additional safeguards, if any.
- Relevant information should include, for example, the assessment on the necessity of the transfer of the specific personal data, an overview of the laws of the third country applicable and the safeguards the importer committed to implement.

Adoption of standards and best practices

135. ***Adoption of strict data security and data privacy policies, based on EU certification or codes of conducts or on international standards (e.g. ISO norms) and best practices (e.g. ENISA) with due regard to the state of the art, in accordance with the risk of the categories of data processed and the likelihood of attempts from public authorities to access it.***

Others

136. ***Adoption and regular review of internal policies to assess the suitability of the implemented complementary measures and identify and implement additional or alternative solutions when necessary, to ensure that an equivalent level of protection to that guaranteed within the EU of the personal data transferred is maintained.***

***

137. ***Commitments from the data importer to not engage in any onward transfer of the personal data within the same or other third countries, or suspend ongoing transfers, when an equivalent level of protection of the personal data to that afforded within the EU cannot be guaranteed in the third country.***[88]

[88] C-311/18 (Schrems II), paragraphs 135 and 137.

ANNEX 3: POSSIBLE SOURCES OF INFORMATION TO ASSESS A THIRD COUNTRY

138. Your data importer should be in a position to provide you with relevant sources and information relating to the third country in which it is established and the laws applicable to it. You may also refer to several sources of information, such as the ones listed below non-exhaustively:

- Case-law of the Court of Justice of the European Union (CJEU) and of the European Court of Human Rights (ECtHR)[89] as referred to in the European Essential Guarantees recommendations;[90]
- Adequacy decisions in the country of destination if the transfer relies on a different legal basis;[91]
- Resolutions and reports from intergovernmental organisations, such as the Council of Europe,[92] other regional bodies[93]; and UN bodies and agencies (e.g. UN Human Rights Council,[94] Human Rights Committee[95]);
- National case-law or decisions taken by independent judicial or administrative authorities competent on data privacy and data protection of third countries;
- Reports from academic institutions, and civil society organizations (e.g. NGOs and trade associations).

[89] See factsheet of the ECtHR jurisprudence on mass surveillance: https://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf
[90] https://www.coe.int/en/web/data-protection/reports-studies-and-opinions
[91] C-311/18 (Schrems II), paragraph 141; see adequacy decisions in https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en
[92] https://www.coe.int/en/web/data-protection/reports-studies-and-opinions
[93] See for instance country reports of the Inter-American Commission on Human Rights (IACHR), https://www.oas.org/en/iachr/reports/country.asp.
[94] See https://www.ohchr.org/EN/HRBodies/UPR/Pages/Documentation.aspx
[95] see: https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/TBSearch.aspx?Lang=en&TreatyID=8&DocTypeID=5



Zalecenie 01/2019 w sprawie projektu wykazu sporządzonego przez Europejskiego Inspektora Ochrony Danych dotyczącego rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych (art. 39 ust. 4 rozporządzenia (UE) 2018/1725)

Przyjęte 10 lipca 2019 r.

Spis treści

1 STRESZCZENIE STANU FAKTYCZNEGO 4
2 OCENA 4
2.1 Ogólne uzasadnienie EROD dotyczące przedłożonego wykazu 4
2.2 Analiza projektu wykazu 5
3 WNIOSEK 8

Europejska Rada Ochrony Danych (EROD)

uwzględniając art. 70 ust. 1 lit. e) rozporządzenia Parlamentu Europejskiego i Rady 2016/679/UE z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (zwanego dalej „RODO"),

uwzględniając art. 39 ust. 4 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725/UE z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE (zwanego dalej „rozporządzeniem 2018/1725"),

uwzględniając art. 12 i 22 swojego regulaminu z dnia 25 maja 2018 r., ze zmianami z dnia 23 listopada 2018 r.,

a także mając na uwadze, co następuje:

(1) Głównym zadaniem EROD jest zapewnienie spójnego stosowania rozporządzenia 2016/679 (zwanego dalej „RODO") na całym terytorium Europejskiego Obszaru Gospodarczego. Zgodnie z art. 70 ust. 1 lit. e) RODO Europejska Rada Ochrony Danych bada w tym celu na wniosek jednego z jej członków wszelkie kwestie dotyczące stosowania tego rozporządzenia i wydaje wytyczne, zalecenia oraz określa najlepsze praktyki, aby zachęcić do jego spójnego stosowania. Art. 39 ust. 6 rozporządzenia 2018/1725 stanowi, że przed przyjęciem projektu wykazu Europejski Inspektor Ochrony Danych zwraca się do EROD o zbadanie – zgodnie z art. 70 ust. 1 lit. e) RODO – takiego projektu wykazu operacji przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych zgodnie z art. 39 ust. 4 rozporządzenia 2018/1725. Obowiązek ten ma zastosowanie w zakresie, w jakim wykaz ten odnosi się do operacji przetwarzania prowadzonych przez administratora danych w rozumieniu art. 3 pkt 8 rozporządzenia 2018/1725, działającego wspólnie z co najmniej jednym administratorem innym niż instytucje i organy Unii. Celem niniejszego zalecenia jest zatem zapewnienie spójności z podejściem przyjętym uprzednio w odniesieniu do projektów wykazów organów nadzorczych (zwanych dalej „organami nadzorczymi"). EROD dążyła do osiągnięcia spójności, po pierwsze – zwracając się do organów nadzorczych o uwzględnienie niektórych rodzajów przetwarzania w swoich wykazach, po drugie – zwracając się do nich o usunięcie pewnych kryteriów, które zdaniem EROD niekoniecznie stwarzają wysokie ryzyko dla osób, których dane dotyczą, i po trzecie – wzywając te organy do stosowania określonych kryteriów w sposób zharmonizowany.

(4) Zgodnie z art. 39 ust. 1 rozporządzenia 2018/1725 dokonanie oceny skutków dla ochrony danych jest dla administratora obowiązkowe wyłącznie w przypadku, gdy przetwarzanie danych „z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych". W art. 39 ust. 3 rozporządzenia 2018/1725 wymieniono, w jakim przypadku istnieje prawdopodobieństwo wystąpienia wysokiego ryzyka. Jest to niewyczerpujący wykaz, który odpowiada brzmieniu art. 35 ust. 3 RODO. W wytycznych dotyczących oceny skutków dla ochrony danych[1], zatwierdzonych przez Europejską Radę Ochrony Danych[2], Grupa Robocza Art. 29 wyjaśniła kryteria, które mogą pomóc w ustaleniu, w jakich przypadkach operacje przetwarzania podlegają wymogowi dokonania oceny skutków dla ochrony danych. W wytycznych Grupy Roboczej Art. 29 nr WP 248 stwierdzono, że w większości przypadków administrator danych może uznać, że dokonania oceny skutków dla ochrony danych wymaga przetwarzanie danych spełniające dwa kryteria. W niektórych przypadkach administrator może jednak uznać, że dokonania tej oceny wymaga przetwarzanie spełniające tylko jedno z tych kryteriów.

(5) Wykazy opracowane przez Europejskiego Inspektora Ochrony Danych mają ten sam cel – określenie operacji przetwarzania, które z dużym prawdopodobieństwem mogą powodować wysokie ryzyko, i operacji przetwarzania, które w związku z tym wymagają dokonania oceny skutków dla ochrony danych. Kryteria opracowane w wytycznych Grupy Roboczej Art. 29 mają zasadniczo zastosowanie.

PRZYJMUJE NINIEJSZE ZALECENIE:

1 STRESZCZENIE STANU FAKTYCZNEGO

1. Zgodnie z art. 39 ust. 4 rozporządzenia 2018/1725 Europejski Inspektor Ochrony Danych przedstawił EROD swój projekt wykazu 18 marca 2019 r., a następnie jego zmienioną wersję 21 czerwca 2019 r.

2. Dokument przedłożony przez Europejskiego Inspektora Ochrony Danych zawierał również część dotyczącą art. 39 ust. 5 rozporządzenia 2018/1725. Zmieniony projekt dokumentu wyraźnie wskazuje, że zawarty w nim wykaz na podstawie art. 39 ust. 5 ma zastosowanie wyłącznie w przypadkach, w których instytucje lub organy Unii są współadministratorami lub jedynymi administratorami. W szczególności projekt wykazu na podstawie art. 39 ust. 5 obejmuje operacje przetwarzania dotyczące przetwarzania danych przez instytucje lub organy Unii do celów ich wewnętrznego zarządzania, prowadzone bez udziału administratorów innych niż instytucje i organy Unii.

3. W związku z tym EROD zwraca uwagę, że ta druga część dokumentu nie wchodzi w zakres stosowania art. 39 ust. 6 rozporządzenia 2018/1725. Przepis ten określa, że obowiązek zwrócenia się do EROD o wydanie zalecenia ma zastosowanie wyłącznie do tych pozycji, które dotyczą operacji przetwarzania, w przypadku których administrator danych podlegający przepisom rozporządzenia 2018/1725 działa wspólnie z co najmniej jednym administratorem innym niż instytucje lub organy Unii. W związku z tym EROD nie będzie komentowała tej części projektu dokumentu.

2 OCENA

2.1 Ogólne uzasadnienie EROD dotyczące przedłożonego wykazu

4. Wykaz przedłożony EROD analizuje się jako szczegółowe rozwinięcie art. 39 ust. 1 rozporządzenia 2018/1725, który to przepis zawsze będzie miał znaczenie rozstrzygające. W związku z tym wspomnianego wykazu nie należy traktować jako wykazu wyczerpującego.

[1] Grupa Robocza Art. 29, Wytyczne dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko" do celów rozporządzenia 2016/679 (WP 248 rev. 01).

[2] EROD, zatwierdzenie 1/2018.

5. EROD zwraca uwagę na art. 39 ust. 10 rozporządzenia 2018/1725, zgodnie z którym nie wymaga się dokonania oceny skutków dla ochrony danych, jeśli dana operacja przetwarzania lub dany zestaw operacji ma podstawę prawną w akcie prawnym przyjętym na podstawie Traktatów, a ocena skutków dla ochrony danych została już przeprowadzona w ramach ogólnej oceny skutków poprzedzającej przyjęcie tego aktu prawnego. W takim przypadku nie ma zastosowania art. 39 ust. 1–6, chyba że dany akt prawny stanowi inaczej.

6. Niniejsze zalecenie zasadniczo nie obejmuje pozycji przedstawionych przez Europejskiego Inspektora Ochrony Danych, które uznano za niewchodzące w zakres art. 39 ust. 6 rozporządzenia 2018/1725. Dotyczy to pozycji, które nie odnoszą się do operacji przetwarzania, w przypadku których administrator działa wspólnie z co najmniej jednym administratorem innym niż instytucje lub organy Unii. Ponieważ jednak Europejski Inspektor Ochrony Danych podjął decyzję o przyjęciu jednego wykazu w odniesieniu do obu tych rodzajów operacji przetwarzania, niniejsze zalecenie stosuje się de facto do obu tych kategorii operacji przetwarzania.

7. Zalecenie ma na celu dostosowanie do podstawowego zestawu operacji przetwarzania, o których umieszczenie w swoich wykazach EROD zwróciła się do wszystkich organów nadzorczych, o ile operacje te nie zostały jeszcze umieszczone w tych wykazach.

8. Oznacza to, że w odniesieniu do ograniczonej liczby rodzajów operacji przetwarzania, które zostaną zdefiniowane w sposób zharmonizowany, EROD zaleca Europejskiemu Inspektorowi Ochrony Danych wprowadzenie wymogu dokonania oceny skutków dla ochrony danych.

9. Jeśli w niniejszym zaleceniu nie ma mowy o określonych pozycjach zawartych w przedłożonym wykazie dotyczącym oceny skutków dla ochrony danych, oznacza to, że EROD nie zwraca się do Europejskiego Inspektora Ochrony Danych o podjęcie dalszych działań.

10. EROD przypomina ponadto, że kluczowe znaczenie dla administratorów danych i podmiotów przetwarzających dane ma przejrzystość. Aby doprecyzować pozycje w wykazie, EROD zaleca zawarcie w wykazach wyraźnych odniesień, w przypadku każdego rodzaju przetwarzania, do kryteriów określonych w wytycznych w celu zwiększenia przejrzystości.

2.2 Analiza projektu wykazu

11. Biorąc pod uwagę, że:

a) art. 39 ust. 1 rozporządzenia 2018/1725 wymaga dokonania oceny skutków dla ochrony danych, jeżeli działalność związana z przetwarzaniem może z dużym prawdopodobieństwem powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych; oraz

b) art. 39 ust. 3 rozporządzenia 2018/1725 zawiera niewyczerpujący wykaz rodzajów przetwarzania, które wymagają oceny skutków dla ochrony danych;

EROD wydaje następujące zalecenia:

Dane wrażliwe

12. W projekcie wykazu wymienia się „dane wrażliwe" jako następujące kryterium: „Dane wrażliwe: dane ujawniające pochodzenie etniczne lub rasowe, poglądy polityczne, przekonania religijne lub światopoglądowe, lub przynależność do związków zawodowych, dane genetyczne, dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej, dane dotyczące stanu zdrowia, seksualności lub orientacji seksualnej, wyroków skazujących i naruszeń prawa lub związanych z nimi środków bezpieczeństwa lub dane w inny sposób uznane za wrażliwe".

13. Mimo że brzmienie jest bardzo podobne do wytycznych (WP 248 rev. 01) dotyczących oceny skutków dla ochrony danych opracowanych przez Grupę Roboczą Art. 29 i zatwierdzonych przez EROD, istnieje pewna istotna różnica. O ile w projekcie wykazu użyto sformułowania „lub dane w inny sposób uznane za wrażliwe", w wytycznych mowa jest o „danych o bardzo osobistym charakterze".

14. EROD zwraca uwagę, że w RODO terminu „dane wrażliwe" nie użyto w żadnym z artykułów, chociaż użyto go w dwóch motywach, przy czym należy go interpretować wyłącznie w odniesieniu do kategorii danych wymienionych w art. 9 i 10 RODO. Aby uniknąć niejasności, EROD zaleca Europejskiemu Inspektorowi Ochrony Danych zmianę sformułowania „lub dane w inny sposób uznane za wrażliwe" i użycie dokładnie tego samego sformułowania, które występuje w wytycznych dotyczących oceny skutków dla ochrony danych.

Przetwarzanie na dużą skalę

15. EROD zwraca uwagę, że Europejski Inspektor Ochrony Danych odwołuje się do wewnętrznej telefonicznej bazy danych należącej do instytucji UE jako negatywnego przykładu przetwarzania na dużą skalę. Niezależnie od tego, czy rzeczywiście wymagana jest ocena skutków dla ochrony danych, nie jest jasne, dlaczego telefoniczna baza danych instytucji UE sama w sobie nie wchodzi w zakres pojęcia przetwarzania na dużą skalę, zwłaszcza że może ona potencjalnie zawierać dane osobowe dużej liczby osób. EROD przypomina również, że pojęcie „na dużą skalę" odnosi się również do odsetka danej populacji, jak określono w wytycznych dotyczących inspektorów ochrony danych, przyjętych w grudniu 2016 r., zmienionych w dniu 5 kwietnia 2017 r. i zatwierdzonych przez EROD. EROD zaleca użycie innego przykładu.

Zbiory danych zestawiane lub łączone z różnych operacji przetwarzania danych

16. EROD zwraca uwagę, że przykład wykorzystany do zobrazowania operacji przetwarzania, w których występują zbiory danych zestawiane lub łączone z różnych operacji przetwarzania danych, może budzić wątpliwości co do jego zgodności z prawem na mocy rozporządzenia 2018/1725, biorąc pod uwagę sposób, w jaki został on przedstawiony. Chociaż EROD nie jest w stanie ocenić tej zgodności z prawem i nie ma do tego kompetencji, zaleca – w celu zapewnienia jasności – podanie innego przykładu.

Osoby, których dane dotyczą, wymagające szczególnej ochrony

17. EROD zwraca uwagę, że Europejski Inspektor Ochrony Danych w swojej decyzji jako przykład negatywny podaje pracowników instytucji UE w odniesieniu do standardowych procedur określonych w regulaminie pracowniczym. EROD przypomina, że w zatwierdzonych przez nią wytycznych Grupy Roboczej Art. 29 dotyczących oceny skutków dla ochrony danych (WP 248 rev. 01) pracownicy są wymienieni jako osoby, których dane dotyczą, wymagające szczególnej ochrony. Chociaż można twierdzić, że brak równowagi sił między pracodawcą a pracownikiem jest mniej rażący w kontekście „standardowych procedur" w ramach odnośnego regulaminu pracowniczego, nie można uznać, że zawsze ma to miejsce, zwłaszcza gdy pracownicy nie mają znaczącego wpływu na treść tego regulaminu. Ponadto nie jest jasne, które procedury można uznać za niestandardowe, w którym to przypadku może być potencjalnie konieczne dokonanie oceny skutków dla ochrony danych, co może

prowadzić do znacznej niejasności. W związku z tym EROD zaleca, by Europejski Inspektor Ochrony Danych zastąpił podany przykład innym.

3 WNIOSEK

18. Rada zwraca się do Europejskiego Inspektora Ochrony Danych o dokonanie następujących zmian w jego wykazie:

- jeśli chodzi o dane wrażliwe: EROD zaleca Europejskiemu Inspektorowi Ochrony Danych zmianę jego wykazu poprzez zmianę sformułowania „lub dane w inny sposób uznane za wrażliwe" oraz zastosowanie dokładnie takiego samego brzmienia jak w wytycznych dotyczących oceny skutków dla ochrony danych;
- jeśli chodzi o dane przetwarzane na dużą skalę: EROD zaleca Europejskiemu Inspektorowi Ochrony Danych zmianę wykazu poprzez wykorzystanie innego przykładu negatywnego;
- jeśli chodzi o zbiory danych zestawiane lub łączone z różnych operacji przetwarzania danych: EROD zaleca Europejskiemu Inspektorowi Ochrony Danych zmianę wykazu poprzez wykorzystanie innego przykładu;
- jeśli chodzi o osoby, których dane dotyczą, wymagające szczególnej ochrony: EROD zaleca Europejskiemu Inspektorowi Ochrony Danych zmianę wykazu poprzez wykorzystanie innego przykładu negatywnego.

W imieniu Europejskiej Rady Ochrony Danych

Przewodnicząca

(Andrea Jelinek)



TABLE OF CONTENTS

1 BACKGROUND 4
2 SCOPE OF THE JOINT OPINION 5
3 ASSESSMENT 7
3.1 General remarks 7
3.2 General issues related to the relationship of the Proposal with Union law in the field of personal data protection 8
3.3 Re-use of certain categories of protected data held by public sector bodies 17
3.3.1 Relationship of the Proposal with the Open Data Directive and with the GDPR 17
3.3.2 Article 5: conditions for re-use of data by public sector bodies 19
3.3.3 Article 5(11): re-use of "highly sensitive" non-personal data 24
3.3.4 Article 6: fees for data re-use 24
3.3.5 Governance and institutional aspects: Article 7 (competent bodies). Article 8 (single information point). 25
3.4 Requirements applicable to data sharing service providers 27
3.4.1 Data intermediaries under Article 9(1) (b): intermediation services between data subjects and potential data users. 30
3.4.2 Data intermediaries under Article 9(1) (c): 'data cooperatives' 32
3.4.3 Article 10: notification regime - general requirements to be eligible for registration - content of the notification; outcome (and timing) of the notification. Article 11: conditions for providing data sharing services 33
3.4.4 Articles 12 and 13: competent authorities and monitoring of compliance (with Articles 10 and 11) 36
3.5 Data altruism 38
3.5.1 Interplay between data altruism and consent under the GDPR 38
3.5.2 Articles 16-17: registration regime - general requirements to be eligible for registration - content of the registration; outcome (and timing) of the registration; 41
3.5.3 Articles 18-19: transparency requirements and "specific requirements to safeguard rights and interests of data subjects and legal entities as regards their data" 42
3.5.4 Articles 20 and 21: competent authorities for registration and monitoring of compliance 44
3.5.5 Article 22: European data altruism consent form. 45
3.6 International transfers of data: Article 5(9)-(13); recital 17, 19; Article 30 45

3.7 Horizontal provisions on institutional settings; complaints; European Data Innovation Board (EDIB) expert group; delegated acts; penalties, evaluation and review, amendments to the single digital gateway regulation, transitional measures and entry into force 47

3.7.1 Article 23: requirements relating to competent authorities 47

3.7.2 Article 24: complaints; Article 25: right to effective judicial remedy 48

3.7.3 Articles 26 and 27: composition and tasks of the European Data Innovation Board Expert Group 48

3.7.4 Article 31: penalties for infringements of the Proposal, to be applied 50

3.7.5 Article 33: amendment to Regulation (EU) 2018/1724 50

The European Data Protection Board and the European Data Protection Supervisor

Having regard to Article 42(2) of the Regulation 2018/1725 of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC ("EUDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,

HAVE ADOPTED THE FOLLOWING JOINT OPINION

1 BACKGROUND

1. The Proposal for Data Governance Act ("the Proposal") is enacted pursuant to the Communication "A European strategy for data" ("the Data Strategy").[1].

2. The European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) notice that, according to the Commission, the Data Strategy provides that "*citizens will trust and embrace data-driven innovation only if they are confident that any personal data sharing in the EU will be subject to full compliance with the EU's strict data protection rules*"[2].

3. As specified in its Explanatory Memorandum, the Proposal "*aims to foster the availability of data for use by increasing trust in data intermediaries and by strengthening data-sharing mechanisms across the EU. The instrument would address the following situations:*

   - Making public sector data available for re-use, in situations where such data is subject to rights of others.

   - Sharing of data among businesses, against remuneration in any form.

   - Allowing personal data to be used with the help of a 'personal data-sharing intermediary', designed to help individuals exercise their rights under the General Data Protection Regulation (GDPR).

   - Allowing data use on altruistic grounds"[3].

4. When presenting the Proposal, the Commission has notably considered *that "the new regulation will provide a good governance framework supporting the common European data spaces and will ensure that data can be made available voluntarily by data holders. It will complement the upcoming rules on*

[1] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions "A European strategy for data", 19 of February 2020, COM (2020) 66 final.
[2] A European strategy for data, Introduction, page 1.
[3] Explanatory Memorandum, page 1.

high-value datasets under the Open Data Directive which will ensure access to certain datasets across the EU for free, in machine-readable format and through standardised Application Programming Interfaces (APIs)"[4].

5. The Data Strategy also highlights that *"The availability of data is essential for training artificial intelligence systems, with products and services rapidly moving from pattern recognition and insight generation to more sophisticated forecasting techniques and, thus, better decisions"*[5].

6. As acknowledged in the Explanatory Memorandum of the Proposal, *"the interplay with the legislation on personal data is particularly important. With the General Data Protection Regulation (GDPR) and ePrivacy Directive, the EU has put in place a solid and trusted legal framework for the protection of personal data and a standard for the world"*[6].

7. The EDPB and the EDPS also point out that the Proposal, as referred to in the Explanatory Memorandum, *"aims at facilitating data sharing including by reinforcing trust in data sharing intermediaries that are expected to be used in the different data spaces. It does not aim to grant, amend or remove the substantial rights on access and use of data. This type of measures is envisaged for a potential Data Act (2021)"*[7]. At the time of drafting this Joint Opinion, the aim and content of such Data Act are not yet available.

2 SCOPE OF THE JOINT OPINION

8. On 25 November 2020, the Commission published the Proposal for a regulation of the European Parliament and of the Council on European data governance ("Data Governance Act") ("the Proposal").

9. On 25 November 2020, the Commission requested a Joint Opinion of the EDPB and the EDPS on the basis of Article 42(2) of Regulation (EU) 2018/1725 (EUDPR) on the Proposal.

10. **The Proposal is of particular importance for the protection of individuals' rights and freedoms with regard to the processing of personal data. The scope of this opinion is limited to the aspects of the Proposal related to the protection of personal data, which, as observed, represent a key -if not the most important- aspect of the Proposal.**

11. In this regard, the EDPB and the EDPS notice that recital (3) provides that "*This Regulation is therefore without prejudice to Regulation (EU) 2016/679*".

12. The EDPB and the EDPS consider that the underlying objective of reinforcing trust with a view to facilitate data availability and benefit the digital economy in the EU is indeed grounded in **the need to ensure and uphold the respect and application of the EU acquis in the field of personal data protection**. Applicable EU law in such field, and in particular Regulation EU 2016/679 (General Data Protection Regulation, GDPR), shall be considered as a prerequisite on which further legislative proposals may build upon without affecting or interfering with the relevant existing provisions, including when it comes to the competence of supervisory authorities and other governance aspects.[8].

13. In the view of the EDPB and the EDPS, it is therefore important to **clearly avoid in the legal text of the Proposal any inconsistency and possible conflict with the GDPR**. This not only for the sake of legal certainty, but also to avoid that the Proposal has the effect of directly or indirectly jeopardizing the fundamental right to the protection of personal data, as established under Article 16 of the Treaty on the Functioning of the European Union (TFEU) and Article 8 of the Charter of fundamental rights of the European Union.

14. In particular, in this Joint Opinion, the EDPB and the EDPS point out to inconsistencies with the EU data protection legislation (as well as with other EU legislation, such as the Open Data Directive) and to problems, relating for instance to legal certainty, that would arise from the entry into force of the current Proposal.

15. Since the Proposal, as detailed in this Joint Opinion, raises a significant number of serious concerns, often intertwined, related to the protection of the fundamental right to the protection of personal data, **it is not the aim of this Joint Opinion to provide an exhaustive list of issues to be addressed by the legislators, nor always alternative proposals or wording suggestions**. Instead, **this Joint Opinion aims at addressing the main criticalities of the Proposal**. At the same time, the EDPB and the EDPS remain available to provide further clarifications and exchanges with the Commission.

16. The EDPB and the EDPS are also aware that the legislative process on the Proposal is ongoing and stress their **availability to the co-legislators to provide further advice and recommendations throughout this process**, to ensure in particular: legal certainty for natural persons, economic operators and public authorities; due protection of personal data for data subjects in line with the TFEU, the Charter of Fundamental Rights of the EU and the data protection acquis; a sustainable digital environment including the necessary 'checks and balances'.

17. This call for the involvement of data protection authorities also relates, due to the possible important links with the Proposal[9], to any forthcoming proposal for a European Data Act.

[4] https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_2103#European%20Data%20Spaces
[5] Data Strategy, pages 2 and 3.
[6] Explanatory Memorandum, page 1.
[7] Explanatory Memorandum, page 1.

[8] See EDPS Opinion 3/2020 on the European strategy for data, at paragraph 64: "Finally, the EDPS underlines that in the context of future governance mechanisms the competences of the **independent supervisory authorities for data protection** must be properly respected. Moreover, the implementation of the Strategy leading to wider use of data will require a **significant increase of resources for DPAs** and other public oversight bodies, in particular in terms of **technical expertise and capabilities**. Cooperation and joint investigations between all relevant public oversight bodies, including data protection supervisory authorities, should be encouraged."

[9] The Impact Assessment accompanying the Proposal, SWD (2020) 295 final, specifies at page 6 that (bold added): "The current initiative is **a first step in the two-step approach** announced in the European Strategy for Data. **The initiative** will address the urgent need to facilitate data sharing through an enabling **governance framework**. **In a second step**, the Commission will address issues about **who controls or 'owns' the data, i.e. the material rights on who can access and use what data under which circumstances**. The **introduction of such rights** will be examined in the context of the **Data Act (2021)**. Diverging interests of the stakeholders and

3 ASSESSMENT

3.1 General remarks

18. The EDPB and the EDPS acknowledge the legitimate objective of fostering the availability of data for use by increasing trust in data intermediaries and by strengthening data-sharing mechanisms across the EU, while highlighting that the protection of personal data is an essential and integral element of the trust individuals and organizations should have in the development of the digital economy. The proposal for a regulation on European Data Governance (Data Governance Act) is also to be considered in the light of the increased reliance of the digital economy on the processing of personal data and of the development of new technologies such as large data set analytics and artificial intelligence.

19. The EDPB and the EDPS underline that, whereas the GDPR was built upon the need to reinforce the fundamental right to data protection, the Proposal clearly focuses on unleashing the economic potential of data re-use and sharing. Thus, the Proposal intends to "improve the conditions for data sharing in the internal market", as stated in Recital (3). However, **the EDPB and the EDPS note that the Proposal, also having regard to the Impact Assessment accompanying it, does not duly take into account the need to ensure and guarantee the level of protection of personal data provided under EU law. The EDPB and the EDPS consider that this policy trend toward a data-driven economy framework without a sufficient consideration of personal data protection aspects raises serious concerns from a fundamental rights viewpoint.** In this regard, the EDPB and the EDPS emphasise that any proposal, including upcoming initiatives related to data, such as the European Data Act, that may have an impact on the processing of personal data, must ensure and uphold the respect and application of the EU acquis in the field of personal data protection.

20. **The EDPB and the EDPS furthermore highlight that the European Union model relies on the mainstreaming of its values and fundamental rights within its policy developments, and that the GDPR must be considered as a foundation on which to build a European data governance model. As already stated in various policy contexts, such as the fight against the COVID-19 pandemic, the EU legal framework in the field of personal data protection shall be considered as an enabler, rather than an obstacle, to the development of a data economy that corresponds to the Union values and principles.**

21. The EDPB and the EDPS trusts this Joint Opinion will inform the co-legislators in ensuring the adoption of a legislative instrument which is fully compliant with the EU acquis in the field of personal data protection and therefore increases trust by upholding the level of protection provided by EU law under the supervision of the independent Data Protection Authorities established under Article 16(2) TFEU.

different views on what is fair in this respect make these issues subject to intense debate, which warrants taking more time."

3.2 General issues related to the relationship of the Proposal with Union law in the field of personal data protection

22. The Proposal contains several references to compliance with the GDPR – which lays down the rules relating to the protection of natural persons with regard to the processing of personal data and to the free movement of personal data (see, among others, recital (3); recital (28) of the Proposal: "*when the data sharing service providers are data controllers or processors in the sense of Regulation (EU) 2016/679 they are bound by the rules of that Regulation*.").

23. The EDPB and the EDPS consider that, in light of the scope of the processing of personal data to which the Proposal makes reference, recital 3 should also include a reference to Directive (EC) 2002/58 ("ePrivacy Directive"), as it is also part of the EU acquis in the field of personal data protection with which the Proposal shall be in compliance, consistent.

24. More in general, the EDPB and the EDPS consider that **both the spirit and the letter of the Proposal must not undermine the level of protection and ensure full consistency with all the principles and rules** established by the GDPR to effectively guarantee the fundamental rights to the protection of personal data provided under Article 8 of the Charter and Article 16 TFEU.

25. Having regard to the above, as referred to in the following paragraphs of this Joint Opinion, the EDPB and the EDPS consider that **the Proposal raises significant inconsistencies with the GDPR**, as well as with other Union law[10], in particular as regards the following five aspects:

(a) Subject matter and scope of the Proposal

(b) Definitions/terminology used in the Proposal;

(c) Legal basis for the processing of personal data;

[10] Although this observation does not strictly relate to the processing of personal data, the EDPB and the EDPS also notice possible confusion and ambiguities as to how the Proposal will apply together with the **Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data in the European Union**. In this regard, it should be pointed out that the definitions of 'processing', 'user', 'professional user', and 'data localization requirement', as well as to other provisions of the Regulation on non-personal data (see for instance Article 6, *Porting of data*), might be not **consistent** or however overlapping with the definitions and the other provisions contained in the Proposal. Moreover, with regards to the re-use of data held by public sector bodies which are protected on grounds of statistical confidentiality, it should be pointed out that, despite the principle stated by Article 3(3) of the Proposal, the conditions for re-use defined in Article 5(3-4) are not in line with the sectoral rules established at EU level for the protection of confidential data used for statistical purposes (see Regulation (EC) No 223/2009 of the European Parliament and of the Council of 11 March 2009 on European statistics and repealing Regulation (EC, Euratom) No 1101/2008 of the European Parliament and of the Council on the transmission of data subject to statistical confidentiality to the Statistical Office of the European Communities, Council Regulation (EC) No 322/97 on Community Statistics, and Council Decision 89/382/EEC, Euratom establishing a Committee on the Statistical Programmes of the European Communities and the Commission Regulation (EU) No 557/2013 of 17 June 2013 implementing Regulation (EC) No 223/2009 of the European Parliament and of the Council on European Statistics as regards access to confidential data for scientific purposes and repealing Commission Regulation (EC) No 831/2002.

(d) Blurring of the distinction between (processing of) personal and non-personal data (and unclear relationship of the Proposal with the Regulation on free flows of non-personal data);

(e) Governance/tasks and powers of competent bodies and authorities to be designated in accordance with the Proposal, having regard to the tasks and powers of data protection authorities responsible for the protection of the fundamental rights and freedoms of natural persons in relation to the processing of personal data as well as for facilitating the free flow of personal data within the Union.

A. Subject matter and scope

26. According to Article 1(2) of the Proposal: "*This Regulation is without prejudice to specific provisions in other Union legal acts regarding access to or re-use of certain categories of data, or requirements relating to processing of personal or non-personal data.*

Where a sector-specific Union legal act requires public sector bodies, providers of data sharing services or registered entities providing data altruism services to comply with specific additional technical, administrative or organisational requirements, including through an authorisation or certification regime, those provisions of that sector-specific Union legal act shall also apply."

27. **For the sake of clarity, the EDPB and the EDPS recommend introducing in Article 1 of the Proposal a provision clearly and unambiguously stating that the Proposal leaves intact and in no way affects the level of protection of individual with regard to the processing of personal data under the provisions of Union and national law and that the Proposal does not alter any obligations and rights set out in the data protection legislation. This addition would provide for better legal certainty and guarantees that fundamental right to the protection of personal data is not undermined.**

28. In this regard it is unclear why a similar specification is contained in Article 9(2) of the Proposal referring to data sharing service providers[11] and not (*mutatis mutandis*, that is referring also to public sector bodies, re-users, data altruism organisations) as a horizontal provision under Article 1 of the Proposal.

B. The definitions of the Proposal are inconsistent with the definitions and key concepts of the GDPR, and therefore need to be amended or clarified

29. The definition of *"data holder"* provided under Article 2(5) of the Proposal: "*the legal person or data subject who, in accordance with applicable Union or national law, has the right to grant access or to share certain personal or non-personal data under its control*" is not in line with the overarching principles of the GDPR, as well as with the letter of the GDPR.

30. In this regard, the EDPB and the EDPS note that legal uncertainties may arise from the fact that the GDPR does not mention the data subject's right to grant access or to share his/her personal data with

[11] Article 9(2) states: "*This Chapter shall be without prejudice to the application of other Union and national law to providers of data sharing services, including powers of supervisory authorities to ensure compliance with applicable law, in particular as regard the protection of personal data and competition law*".

third parties and even less so an equivalent right for the legal person which seems possible to extrapolate from the definition of "data holder". Rather, the GDPR guarantees to every individual the right to the protection of personal data concerning him or her, which refers to a comprehensive set of rules for the processing of personal data that are binding for each entity processing the data (data controller/joint controller) or processing the data on behalf of the data controller (processor)[12].

31. **In this regard, the EDPS and the EDPB believe that rather than stating that a legal person has the right to grant access to or share personal data, it would be more appropriate referring to whether and under which conditions a certain processing of personal data can be performed or not.**

32. A clarification that the EDPB and the EDPS would like to make is that both the access to and the sharing of personal data constitute processing of personal data pursuant to Article 4(2) of the GDPR.

33. According to the data protection legislation, the processing of personal data shall be lawful if the data subject (the identified or identifiable natural person to whom personal data relate) has given consent to the processing of his or her personal data for one or more specific purposes or if another adequate legal basis under Article 6 GDPR can be validly applied.

34. The aforesaid considerations are made in the light in particular of Article 8 of the Charter: "*1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law.*"

35. The EDPB and the EDPS have concerns also as regards the wording of recital (14) of the Proposal (underline added): "*Companies and data subjects should be able to trust that the re-use of certain categories of protected data, which are held by the public sector, will take place in a manner that respects their rights and interests.*"; Article 11(6), referring to "*guarantees in place that allow data holders and data users to obtain access to their data in case of insolvency*"; as well as of Article 19, "*Specific requirements to safeguard rights and interests of data subjects and legal entities as regards their data*", which refers under Article 19(1)(a) to: "*the purposes of general interest for which it [any entity entered in the register of recognised data altruism organisations] permits the processing of their data [of data holders] by a data user*".

36. In this regard, the EDPB and the EDPS remark that rights and interests of the data subject with regard to his or her personal data, on the one hand, and the right and interests of legal persons with regard

[12] See also recital (6) and (7) of the GDPR (bold added):
"(6) Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Natural persons increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life, and should further facilitate the free flow of personal data within the Union and the transfer to third countries and international organisations, while ensuring a **high level of the protection of personal data**.
(7) Those developments require a **strong and more coherent data protection framework** in the Union, backed by **strong enforcement**, given the importance of creating the **trust** that will allow the digital economy to develop across the internal market. **Natural persons should have control of their own personal data**. **Legal and practical certainty** for natural persons, economic operators and public authorities should be enhanced."

to the information relating to them, on the other hand, are not of the same kind (the latter does not concern human dignity or the right to privacy and to data protection, but rather industrial property rights, such as trade secrets, patents and trademarks). Therefore, given the aforesaid heterogeneity, the mentioned provisions would be not only not conceptually 'solid', but also difficult to implement and such as to raise legal uncertainties. For instance, in case of insolvency (referred to under Article 11(6)), the guarantees in place to allow data holders to obtain access to non-personal data would differ substantially in practice from conditions and limits for the continued processing of personal data. These are indeed different issues that require different solutions[13], and the reference to both under the obligation for the data sharing service provider to ensure continuity of provision of services (including the sharing of personal data) is confusing at least, if not manifestly inconsistent with the GDPR.

37. The definition of 'data user'[14] under Article 2(6) is also a new definition introduced by the Proposal, whose interplay -in case of personal data- with the definition of recipient[15] under Article 4(9) of the GDPR is unclear. We note in this regard that Article 11(1) of the Proposal lays down: "The provider may not use the data for which it provides services for other purposes than to put them at the disposal of data users […]" This provision, read in conjunction with the definition of 'data user', gives rise to legal uncertainty, due to different notions of *'recipient'* under GDPR and *'data user'* under the Proposal, which would lead to difficulties of practical application. Moreover, the definition under Article 2(6) might be misleading if read as referring to a natural or legal person that is authorised (has the right?) to use personal data for commercial and non-commercial purposes. The reference to and the meaning (its legal source and effect) of such "authorization" is also unclear.

38. In addition, the interplay between the notion of data user as "natural or legal person [authorised to use data for commercial and non-commercial purposes]" and the notions of controller, joint controller or processor under the GDPR is also unclear. Furthermore, the Proposal refers to a possible qualification as controller or processor and their obligations under the GDPR for the data sharing service providers[16], but not for the data user or for the data altruism organisations (despite the fact that the latter can also be controller, joint controller or processor under the GDPR).

39. **More in general, the EDPB and the EDPS underline that the Proposal should define the roles in respect of personal data protection law (data controller, processor or joint controller) of each type of 'actor' (data sharing service provider, data altruism organisation, data user) not only to avoid ambiguity about the applicable GDPR obligations, but also to improve the readability of the legal text.**

40. Similar issues, namely the **unclear relationship with the definitions and rules provided under the GDPR**, relate to the definition of 'data sharing' under Article 2(7) of the Proposal (referring *inter alia* to the 'joint or individual use of the shared data'). Insofar as it relates to personal data, the joint use of personal data (by both the data holder, legal person, and a data user) directly or through an intermediary, is also confusing at least.

41. Similar concerns - as further detailed below - relate to the term "permission [from legal entities to the reuse of data]", for which however a definition is not provided in the Proposal.

42. The definition of 'metadata' in Article 2(4) is also problematic under the personal data protection viewpoint, since it refers to "data collected on any activity of a natural or legal person for the purposes of the provision of a data sharing service, including the date, time and geolocation data, duration of activity, connections to other natural or legal persons established by the person who uses the service". Such data may include personal data.

43. As further detailed in this Joint Opinion, having regard to Article 11(2), the Proposal may be interpreted as creating a legal basis for the processing of metadata. Article 11 of the Proposal seems to lay down that, as a condition for providing the data sharing service, the provider should indeed be able to use the aforesaid metadata "for the development of that [the data sharing] service". No reference is made in the legal text among others to the need for the data sharing service provider to rely upon an appropriate legal basis for processing of personal data under Article 6(1) of the GDPR.

44. **More in general, the EDPB and the EDPS consider that since the Proposal is, as made explicit in the Proposal itself, without prejudice to the GDPR, the definitions envisaged by the GDPR should apply and they should not be implicitly amended or removed by the Proposal and the new definitions, as far as they relate to the processing of personal data, should not, as 'a matter of fact', contain 'rules' that are inconsistent with the spirit and the letter of the GDPR.**

45. This specification is particularly important due to the cumulative effect in terms of lack of clarity and legal uncertainties arising from the Proposal where more than one unclear definition is contained in the same provision (see for instance Article 7(2)(c) of the Proposal, referring to "obtaining consent *or* permission by re-users for re-use for altruistic and other purposes in line with specific decisions of data holders").

46. **In light of the above, the EDPB and the EDPS recommend clarifying and modifying the Proposal in order to ensure that -insofar as personal data are concerned- no inconsistencies with the definitions and concepts of the GDPR remain.**

C. The Proposal should better specify, to avoid legal uncertainties, the applicable legal basis in the GDPR for the processing of personal data

47. The EDPB and the EDPS notice that the Proposal makes reference to "the permission of data holders" for the use of data under several provisions:

[13] For instance, in case of insolvency, attention should be paid to the fact that, as a result, there is a change in the controllership of the data processing. The new controller shall establish in particular what data can be processed; identify the purposes for which the data was originally obtained; establish the lawful basis for sharing the data; ensure compliance with the data protection principles, in particular lawfulness, fairness and transparency; inform data subjects about changes relating to the processing of their data, and consider that data subjects may exercise their right to object.

[14] Article 2(6) of the Proposal: "'**Data user**' means **a natural or legal person** who has lawful access to **certain** data and is **authorised to use that data** for commercial or non-commercial purposes."

[15] According to the definition provided in the GDPR, under Article 4(9), "'recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not […]".

[16] See recital 28 "where the data sharing service providers are data controllers or processors in the sense of the Regulation (EU) 2016/679 they are bound by the rules of that Regulation."

- Article 5(6): "*the public sector body shall support re-users in seeking consent of the data subjects and/or permission from the legal entities whose rights and interests may be affected by such re-use", specified under recital (11): "The public sector bodies, where relevant, should facilitate the re-use of data on the basis of consent of data subjects or permissions of legal persons on the re-use of data pertaining to them through adequate technical means."*

- Article 7(2)(c): *"assisting the public sector bodies, where relevant, in obtaining consent or permission by re-users for re-use for altruistic and other purposes in line with specific decisions of data holders [..]";*

- Article 11(11): *"where a provider provides tools for obtaining consent from data subjects or permissions to process data made available by legal persons";*

- Article 19(3): *"Where an entity entered in the register of recognised data altruism organisations provides tools for obtaining consent from data subjects or permissions to process data made available by legal persons", specified under recital (36) "Legal persons could give permission to the processing of their non-personal data for a range of purposes not defined at the moment of giving the permission."*

48. The EDPB and the EDPS notice in this regard that it is unclear in most cases whether the object of the permission would be the re-use of personal or non-personal data or both.

49. The EDPB and the EDPS also remark that in case of processing of personal data **the "permission" referred to in the Proposal cannot replace the necessity of one appropriate legal ground under Article 6(1) of the GDPR for the lawful processing of personal data**. In other words, according to the GDPR the processing of personal data shall be lawful only if and to the extent that at least one of the legal basis under Article 6(1) of the GDPR applies. The Proposal should clearly specify this aspect to avoid any ambiguity.

50. Indeed, even interpreting the notion of 'permission', (to be however defined in the legal text of the Proposal) as 'a decision (a business choice) by a legal person to permit the processing of personal data where such legal person has a legal basis under Article 6(1) of the GDPR to permit such processing', it has to be noted that the literal reading of some provisions of the Proposal does not seem to support this GDPR-compliant interpretation, since they refer for instance to "*Where the re-use of data cannot be granted in accordance with the obligations laid down in paragraphs 3 to 5 and there is no other legal basis for transmitting the data under Regulation (EU) 2016/679, the public sector body shall support re-users in seeking consent of the data subjects and/or permission from the legal entities*" (Article 5(6) of the Proposal)[17]. In these cases, 'permission' seems to be alternative to at least one (consent of the data subject) of the legal basis provided under Article 6 of the GDPR.

51. Recital 6 of the Proposal is also unclear with regard to the appropriate legal basis for the processing of personal data, since it refers to an obligation "in general" to rely on the legal basis provided in Article 6 of the GDPR for the processing of personal data[18].

[17] See also Article 7(2)(c); Article 11(11); Article 19(3) of the Proposal referred to above

[18] In particular, recital 6 of the Proposals states that (bold added): "**In general**, insofar as personal data are concerned, the processing of personal data should rely upon one or more of the grounds for processing provided in Article 6 of Regulation (EU) 2016/679."

52. From another standpoint, as a further detailed in this Opinion, the EDPB and the EDPS remark the need to **clarify the relationship between the different scenarios envisaged under the Proposal and Article 6(4) of the GDPR**, regulating the situation where the processing of personal data for a purpose other than that for which the personal data have been collected is not based on the data subject's consent.

53. **To that effect, in light of the objective and content of the Proposal, the EDPB and the EDPS consider that the Proposal cannot be invoked as Union law constituting a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1) of the GDPR in order to ground the processing for a purpose other than that for which the personal data has been initially collected, where such processing is not based on consent, as per Article 6(4) of the GDPR.**

54. **Also in light of the above, the EDPB and the EDPS recommend specifying in the legal text of the Proposal that insofar as personal data are concerned, their processing must always be based on an adequate legal basis under Article 6 of the GDPR.**

55. As an example of possible inconsistency relating to the legal basis for the processing of personal data, we point out to the provision under Article 11(2) of the Proposal, according to which *"the metadata collected on the basis of the data sharing offered may be used [only] for the development of the data sharing services"*. In this regard, we recall that metadata referred to in the Proposal[19] can constitute information relating to an identified or identifiable natural person and in this case must be processed in accordance with data protection rules and, in particular, those concerning the legal basis of the processing. However, as referred to in paragraph 51 of this Opinion, this essential aspect is not addressed by the Proposal.

56. **On this matter, as a broader observation, the EDPB and the EDPS consider that the aforesaid provision, as well as any other provision of the Proposal, does not provide a self-standing legal basis for the re-use of personal data by data users and for the processing activities performed by providers of data sharing services or by data altruism organisations, due to the fact that it does not fulfil the criteria under Article 6(3) for the processing referred to in point (c) and (e) of Article 6(1)[20] of the GDPR.**

[19] Under Article 2(4) of the Proposal "'metadata' means data collected on any activity of a natural or legal person for the purposes of the provision of a data sharing service, including the date, time and geolocation data, duration of activity, connections to other natural or legal persons established by the person who uses the service."

[20] "3. The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:
(a) Union law; or (b) Member State law to which the controller is subject.
The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations as provided for in Chapter IX. The Union or the

D. Blurring of the distinction between (processing of) personal and non-personal data and unclear relationship of the Proposal with the Regulation on free flows of non-personal data

57. As a general remark, the EDPB and the EDPS consider that a main criticality of the Proposal, having regard to the protection of personal data, possibly at the origin of the aforesaid incompatibilities or at least ambiguity of the legal text, is the blurring of the distinction between the processing of non-personal data, as regulated for certain aspects under Regulation (EU) 2018/1807 of 14 November 2018 on a framework for the free flow of non-personal data in the European Union ("Regulation on the free flow of non-personal data)"[21], and the processing of personal data, the latter regulated under the data protection acquis and inspired by different principles.

58. In this regard, the EDPB and the EDPS underline that the distinction between categories of personal and non-personal data is difficult to apply in practice. Indeed, in practice, from a combination of non-personal data it is possible to infer or generate personal data, i.e. data relating to an identified or identifiable individual[22], especially when non-personal data are the result of the anonymisation of personal data and thus information originally related to natural persons. In addition, in the scenarios envisaged by the Proposal of increased availability, re-use and sharing of information, with a view to "allowing 'Big Data' pattern detection or machine learning"[23], the more non-personal data are combined with other available information, the more difficult it will be to ensure anonymisation because of the increased re-identification risk for data subjects. Consequently, having this scenario in mind, the data subjects' fundamental rights to privacy and data protection should be ensured in any case in the different contexts envisaged by the Proposal.

59. At the same time, there might be cases of non-personal data, to which the GDPR does not apply, that since their origin, do not relate to naturals persons. For instance, it is the case of non-personal data from vibration sensors in industrial machinery combined with other non-personal data, e.g. the geolocation of the machinery. Such non-personal data does not need the same level of safeguards than non-personal data that are the result of the anonymisation of personal data, as only the latter (likewise pseudonymised data) are likely to be exposed to the risk of re-identification.

60. **To avoid confusion as to how the Proposal would apply 'together with the GDPR', the EDPB and the EDPS recommend reworking the Proposal taking better into account the distinction between personal and non-personal data as well among different types of non-personal data.**

Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued."

[21] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (Text with EEA relevance.), OJ L 303, 28.11.2018, p. 59–68.

[22] See EDPS Opinion 3/2013 on the European strategy for data at para 30.

[23] Explanatory Memorandum, page 3.

61. Therefore, notwithstanding the concerns already expressed by the EDPS with regard to the concept of mixed dataset and to "inextricably linked" personal and non-personal data[24], the EDPB and the EDPS recall that, according to Article 2(2) of the Regulation on the free flow of non-personal data: "*In the case of a data set composed of both personal and non-personal data, this Regulation applies to the non-personal data part of the data set. Where personal and non-personal data in a data set are inextricably linked, this Regulation shall not prejudice the application of Regulation (EU) 2016/679*." Consequently, a mixed dataset will as a rule be subject to the obligations of data controllers and processors and the data subject's rights established by the GDPR. This consideration is particularly relevant in the context of the Proposal, since it is possible that in most cases datasets shared through a data sharing service provider or a data altruism organisation would also contain personal data. Since a 'third category' between personal and non-personal data does not exist, this would not change the nature and the 'legal regime' of the dataset as personal data[25].

62. **In the light of the above, the EDPB and the EDPS point out to the risk that the Proposal creates a parallel set of rules, which are not consistent with the GDPR, nor with the Regulation on the free flow of non-personal data, thus undermining it and causing difficulties of practical application.**

E. Governance/tasks and powers of competent bodies and authorities to be designated in accordance with the Proposal and tasks and powers of the data protection authorities

63. The Proposal foresees the designation by Member States of competent bodies to support the public sector bodies which grant access to the re-use of data (Chapter II of the Proposal) and the designation of competent authorities to monitor the compliance with the provisions related to data sharing services and data altruism (Chapters III and IV of the Proposal).

64. **As a broader remark, the EDPB and the EDPS are of the opinion that, since many of the tasks of the competent bodies and authorities under the Proposal relate to the processing of personal data, there is a risk of interferences by the competent bodies and authorities designated under the Proposal with the competence and tasks of independent data protection authorities. Therefore, the designation of competent authorities/bodies other than data protection authorities could lead to real complexity for digital players and data subjects, and also affect consistency in terms of monitoring the application of the provisions of the GDPR. The designation of competent bodies and authorities being left at the discretion of Member States, there may also be a risk of inconsistency and divergence in regulatory approaches across the Union.**

[24] See the Comments of the EDPS on a Proposal for a Regulation of the European Parliament and of the Council on a framework for the free-flow of non-personal data in the European Union issued on the 8th June 2018 at https://edps.europa.eu/sites/edp/files/publication/18-06-08-edps_formal_comments_freeflow_non_personal_data_en.pdf.

[25] See also Communication from the Commission to the Council and to the European Parliament, *Guidance on the Regulation on a framework for the free flow of non-+persona data in the European Union*, at: https://ec.europa.eu/digital-single-market/en/news/guidance-regulation-framework-free-flow-non-personal-data-european-union

3.3 Re-use of certain categories of protected data held by public sector bodies

3.3.1 Relationship of the Proposal with the Open Data Directive and with the GDPR

65. While the Explanatory Memorandum states that the Proposal *"complements the Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (Open Data Directive)*[26]*"*, recital (5) further specifies that *"Directive (EU) 2019/1024 as well as sector-specific legislation ensure that the public sector makes more of the data it produces easily available for use and re-use. However, certain categories of data (commercially confidential data, data subject to statistical confidentiality, data protected by intellectual property rights of third parties, including trade secrets and personal data not accessible on the basis of specific national or Union legislation, such as Regulation (EU) 2016/679 and Directive (EU) 2016/680) in public databases is often not made available, not even for research or innovative activities. Due to the sensitivity of this data, certain technical and legal procedural requirements must be met before they are made available, in order to ensure the respect of rights others have over such data. Such requirements are usually time- and knowledge-intensive to fulfil. This has led to the underutilisation of such data. While some Member States are setting up structures, processes and sometimes legislate to facilitate this type of re-use, this is not the case across the Union."*

66. The EDPB and the EDPS observe that, despite the aforesaid specifications, the interface of the Proposal with the "Open Data Directive" seems unclear. In particular, there might be legal uncertainty on the extended re-use of public sector information, which, according to Article 3 (Scope of application) of the Proposal, would apply to:

"[..]data held by public sector bodies which are protected on grounds of:

(a) commercial confidentiality;

(b) statistical confidentiality;

(c) protection of intellectual property rights of third parties;

(d) protection of personal data."

67. The Explanatory Memorandum to the Proposal[27] does not sufficiently clarify the scope of such extended re-use and the interplay of the Proposal with the Open Data Directive. Moreover, it puts under the same 'umbrella' (as "*respect of rights of others*", which is inappropriate having regard to the protection of personal data) "*protection of personal data, but also protection of intellectual property rights and commercial confidentiality*".

68. It can be argued that the wording "*data held by public sector bodies which are protected on the grounds of*", among others "*protection of personal data*" (Article 3, letter (d)) is at the same time:

- regrettable, since it suggests the idea of data protection regulation as *impeding* the free movement of personal data, rather than laying down the rules of free flow of personal data while protecting the rights and interests of the persons concerned; *and*

- partially inaccurate, since the Open Data Directive, rather than excluding personal data from its scope[28], provides, under Article 1(2)(h), that [the Open Data Directive does not apply to] "*documents, access to which is excluded or restricted by virtue of the access regimes on grounds of protection of personal data, and parts of documents accessible by virtue of those regimes which contain personal data the re-use of which has been defined by law as being incompatible with the law concerning the protection of individuals with regard to the processing of personal data or as undermining the protection of privacy and the integrity of the individual, in particular in accordance with Union or national law regarding the protection of personal data*"[29].

69. This last aspect is however specified under recital 7 of the Proposal[30]. In this regard, the EDPB and the EDPS wonder why this important issue (as well as many others concerning the protection of personal data) is included in a recital, but not in the substantive part of the Proposal.

70. Moreover, pursuant to Article 3(1) of the Open Data Directive, personal data that do not fall under this exception, being freely accessible according to the Union or national access regimes and re-usable for compatible uses without undermining the protection of privacy and the integrity of the individual, are within the scope of the Directive and can be made available for re-use in accordance to the conditions set out in the same Directive as well as in compliance to the requirements of data protection law . Indeed, as stated in recital 154 of the GDPR, the EU legislation on the re-use of public sector information *"leaves intact and in no way affects the level of protection of natural persons with regard to the processing of personal data under the provisions of Union and Member State law, and in particular does not alter the obligations and rights set out in [the GDPR]"*. To this effect, the EU legislator when establishing new principles and rules for the re-use of public sector information should provide for the necessary reconciliation of such re-use with the right to the protection of personal data pursuant to the GDPR[31].

71. **Consequently, the EDPB and the EDPS underline that the rules of the Open Data Directive along with those of the GDPR provide already for mechanisms allowing the sharing of personal data held by**

[26] OJ L 172, 26.6.2019, p. 56–83.

[27] See at page 7: *"Chapter II creates a mechanism for* ***re-using certain categories of protected public sector data,*** *which is* ***conditional on the respect of rights of others*** *(notably on grounds of protection of personal data, but also protection of intellectual property rights and commercial confidentiality). This mechanism is without prejudice to sector-specific EU legislation on access to and the re-use of this data.* ***The re-use of such data falls outside the scope of Directive (EU) 2019/1024*** *(Open Data Directive). Provisions under this Chapter do not create right to re-use such data, but provide for a set of harmonized basic conditions under which the reuse of such data may be allowed (e.g. the requirement of non-exclusivity)."*

[28] See Article 1 of the Open Data Directive.

[29] See also in this regard, recital 52 and 53 as well as Articles 1(4) and 10 of the Open Data Directive, the latter with specific reference to research data.

[30] *"The data covered by this Regulation* ***fall outside the scope of Directive (EU) 2019/1024*** *that excludes data subject to commercial and statistical confidentiality and data for which third parties have intellectual property rights.* ***Personal data fall outside scope of Directive (EU) 2019/1024 insofar as the access regime*** *excludes or restricts access to such data for reasons of privacy and the integrity of the individual, in particular in accordance with data protection rules."* (emphasis added).

[31] See recital 154 as well as Article 86 of the GDPR with specific reference to Union and Member State law on public access to official documents

the public sector bodies in a manner consistent with the requirements governing protection of individuals' fundamental rights. Thus, the EDPB and the EDPS recommend to align Chapter II of the Proposal with the existing rules on the protection of personal data laid down in the GDPR and with the Open Data Directive, so as to ensure that the level of personal data protection in the EU is not undermined and to avoid, at the same time, that these misalignments generate legal uncertainty for individuals, public sector bodies and re-users. As an alternative, without prejudice to the further indications in this Joint Opinion about the impact on the individuals' right to privacy and data protection of the rules of the Proposal governing the re-use of certain categories of protected data held by public sector bodies, personal data could be excluded from its scope.

3.3.2 Article 5: conditions for re-use of data by public sector bodies

72. The conditions for re-use of data held by public sector bodies are provided under Article 5 of the Proposal as specified under recital 11. In this regard, the EDPB and the EDPS consider that the Proposal raises some concerns.

73. **The EDPB and the EDPS reiterate that all processing of personal data as referred to in the Proposal shall occur in full compliance with the GDPR, and thus accompanied by appropriate data protection safeguards. This means that the re-use of personal data should always respect the principles of lawfulness, fairness and transparency as well as purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality in line with Article 5 of the GDPR.**

74. In this scenario, fairness, transparency and purpose limitation are essential safeguards to bring trust among individuals whose personal data are held by the public sector, making them confident that the re-use of the information they provide will take place in a manner that respects their rights and interests (see recital 14 of the Proposal), i.e., that their personal data will not be used against them in an unexpected manner. The importance of the principle of purpose limitation is clearly demonstrated in the context of the measures that are being considered to fight against the COVID-19, e.g. health data to be processed under the control of healthcare authorities as data controllers and not to be used for commercial or other incompatible purpose[32]. Consequently, public sector bodies which are competent under national or EU law to grant or refuse access for the re-use must take into account that the re-use of personal data is permissible only if the principle of purpose limitation as set out in point (b) of Article 5(1) and Article 6 of the GDPR is met[33]. Any subsequent use of data, collected and/or shared in pursuit of a public task (e.g. for improving transport/mobility or tackling serious cross-border threats to health), for commercial for-profit purposes (for instance insurance, marketing, etc.) should be avoided. Such "function creep" might not only constitute a breach of the data protection principles under Article 5 of the GDPR, but could also undermine the trust of individuals in the re-use mechanism, which is a fundamental aim of the Proposal (see recitals 14 and 19)[34].

75. In this regard, the EDPB and the EDPS recall that Article 6(4) GDPR clarifies the concept of 'compatible further processing' (of personal data). Indeed, according to the definition of 're-use' set out in Article 2(2) of the Proposal, when it concerns personal data, the re-use is to be regarded, under a data protection perspective, as a further processing of personal data held by public sector bodies for

[32] See EDPS Opinion on the European Strategy for Data, paragraph 10.
[33] See in this regard recital (52) of the Open Data Directive.
[34] See EDPS Opinion on the European Strategy for Data, paragraph 25.

subsequent not well described (commercial or non-commercial) purposes. However, Article 5 of the Proposal, concerning the conditions for re-use, does not provide any indication on the purposes for which the re-use may be lawfully authorised, nor it specifies that the purposes of any subsequent re-use have to be carefully identified and clearly defined in Union or Member State law in compliance with Article 6(1)(c) or 6(1)(e) and 6(3) of the GDPR[35], eventually satisfying the requirements of Article 23(1) of the GDPR pursuant to Article 6(4) of the GDPR[36].

76. More generally, the Proposal does not seem to lay down any legal obligation for public sector bodies to make data they held available for re-use, nor does it explicitly aim at safeguarding the objectives listed in Article 23 of the GDPR.

77. **Therefore, the EDPB and EDPS strongly recommend to amend the Proposal so as to clarify that the re-use of personal data held by public sector bodies may only be allowed if it is grounded in Union or Member State law which lays down a list of clear compatible purposes for which the further processing may be lawfully authorised or constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23 of the GDPR**.

78. **Furthermore and in line with the above recommendation, to allow a lawful access to personal data by "data users", as indicated by the definition of 'data users' pursuant to Article 2(6) of the Proposal, public sector bodies, which are competent under national or EU law to grant or refuse such access for the re-use, must rely on an adequate legal basis under Article 6 of the GDPR being applicable to the said disclosure. However, this aspect is not specified under Article 5 of the Proposal referring to the conditions for re-use of personal data held by public sector bodies.**

79. Indeed, recital 11 of the Proposal and the corresponding Article 5(3)-(6) does not refer to Union or Member State law that would provide the legal basis under Article 6(1)(c) or (e) of the GDPR, but lays down (bold added): "*In particular, personal data should only be transmitted for re-use to a third party where a legal basis allows such transmission*". In this respect, it shall be noted that the reference should be to the legal basis "under the GDPR". Moreover, the said recital restricts itself to state that "*[t]he public sector bodies, where relevant, should facilitate the re-use of data on the basis of consent of data subjects or permissions of legal persons on the re-use of data pertaining to them through adequate technical means. In this respect, the public sector body should support potential re-users in seeking such consent by establishing technical mechanisms that permit transmitting requests for*

[35] According to Article 6.3 GDPR, Union or Member State law under Article 6(1)(c) or 6(1)(e) of the GDPR should identify amongst other elements the "purpose limitation" of the personal data processing as well as the "purpose for which data may be disclosed".
[36] In another respect, the inclusion of data held by public sector bodies which are protected on grounds of statistical confidentiality in the scope of Chapter II of the Proposal, according to its Article 3(1)(b) and despite the principle stated in its Article 3(3), risks to contradict, the essential principles of data protection in the statistical sector and in particular, the purpose limitation principle, which strictly prohibits the use of confidential data for purposes that are not exclusively statistical, thus undermining trust of natural persons in providing their personal data for statistical purposes (see recital 27 of the above mentioned Regulation (EC) No 223/2009 on European statistics and Articles 4(1) and 4(2) of the Recommendation of the Council of Europe No R (97)18 concerning the protection of personal data collected and processed for statistical purposes).

consent from re-users, where practically feasible. No contact information should be given that allows re-users to contact data subjects or companies directly."

80. The wording of recital 14 of the Proposal is also unclear in setting out the interplay of this Chapter of the Proposal with the GDPR: *"[…] Additional safeguards should thus be put in place for situations in which the re-use of such public sector data is taking place on the basis of a processing of the data outside the public sector. Such an additional safeguard could be found in the requirement that public sector bodies should take fully into account the rights and interests of natural and legal persons (in particular the protection of personal data, commercially sensitive data and the protection of intellectual property rights) in case such data is transferred to third countries"*[37].

81. **Furthermore, the EDPB and the EDPS notice that Article 5(6) of the Proposal lays downs "Where the re-use of data cannot be granted in accordance with the obligations laid down in paragraphs 3 to 5 and there is no other legal basis for transmitting the data under Regulation (EU) 2016/679 […]". In this regard, the EDPB and the EDPS are of the opinion that the conditions listed under paragraphs 3 to 5 (among which, access and re-use of data within a secure processing environment) cannot be considered as an alternative to the legal basis exhaustively listed under Article 6 of the GDPR, unless the reference to (Union or) Member State law is made in the aforesaid paragraphs[38].**

82. In addition, it is unclear the role of the public sector body in supporting re-users in obtaining the consent for the reuse by the data subject. As a further remark on Article 5(6) of the Proposal, the EDPB and the EDPS point out that this provision establishes an obligation for public sector bodies ("shall support"), whose content is not well defined. More to the point, the legal basis under the GDPR for contacting data subjects to collect their consent for the re-use should be specified, as well as the respective responsibility related to obtaining a valid consent under Article 7 of the GDPR.[39] In this regard, it should also be taken into account the clear imbalance of power which is often present in the relationship between the data subject and the public authorities[40]. In this context, in line with the GDPR accountability principle, the EDPB and the EDPS recall that the choice of an appropriate legal basis for the processing of personal data, as well as the demonstration that the chosen legal basis (in this case consent) can be validly applied, lies on the data controller.

83. **Therefore, in line with the principle of lawfulness established by the GDPR, the EDPB and EDPS strongly recommend to clarify, among the conditions for re-use provided for in Article 5 of the Proposal, that an appropriate legal ground under GDPR must be provided in Union or Member State law and carefully identified by public sector bodies with regard to any subsequent re-use of personal data.**

[37] In addition, the EDPB and EDPS note that public sector bodies should not just take into account but **comply with** the legal framework protecting the rights and interests of data subjects.
[38] It might also be worth specifying, for the sake of clarity, that intellectual property rights, referred to under Article 5(7), do not allow (constitute a legal basis for) the processing of personal data.
[39] Would it be the responsibility of the public sector body or of the re-user?
[40] In another respect, it should be reminded that consent in most cases is not an appropriate legal basis for the processing activities performed by public authorities. See the EDPB Guidelines 5/2020 on consent under Regulation 2016/579 at https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en

84. Other key elements to build the level of trust aimed at in the Proposal are the fairness and the transparency principles. According to these principles, individuals must be fully aware whether the personal data they provide to the public sector bodies, or that are further processed by the same bodies in the pursuit of their public tasks, will become subject to re-use and for which purposes, as well as the recipients or categories of recipients to whom the personal data will be disclosed taking into account that in most cases data subjects are compelled under national law to provide their personal data to public bodies because of legal obligations or because they apply for a public action or service[41].

85. However, among the conditions for re-use established in Article 5 of the Proposal, there is no reference to the obligations for the public sector bodies of informing the data subjects under the GDPR, nor to the need of involving them in the process of enabling the re-use of their personal data. This not only undermines the principles of fairness and transparency established by the GDPR to ensure that individuals have a clear overview and control on the possible uses of their own personal data, but also contradicts the same goals of the Proposal which is to increase trust of data subjects that the re-use "will take place in a manner that respects their right and interests" [42]. **Therefore, the EDPB and EDPS recommend to include in the Proposal an explicit reference to the obligations for the public sector bodies of informing the data subjects under the GDPR so that to foster the exercise of the rights conferred to them by the data protection legislation, especially the right to object pursuant to Article 21 of the GDPR. In this respect, the EDPB and EDPS also recommend to define in the Proposal adequate means by which individuals may participate, in an open and collaborative manner, in the process of allowing the re-use of their personal data.**

86. Moreover, to attain a reasonable level of trust in the re-use mechanism, public sector bodies, competent under national or EU law to allow access for the re-use must respect the principles of data minimisation and consider the special protection required for specific sectors routinely dealing with special categories of personal data, such as the health sector, when they establish the scope and conditions for allowing access for the re-use. In assuming these decisions, accuracy, storage limitation, integrity and confidentiality of personal data should also be carefully considered, as well as the potential impact on the concerned data subjects.

87. **In this regard, the EDPB and EDPS call the attention of the legislator to the need of addressing the necessary requirements of the protection of personal data, especially in "sensitive sectors" such as the health sector, when establishing the rules governing the re-use of personal data, as well as the related conditions and specific data protection safeguards.**

88. In particular, according to the GDPR, the data protection impact assessment (DPIA) is a key tool to ensure that data protection requirements are properly taken into account and the rights and interests of individuals are adequately protected, so as to foster their trust in the re-use mechanism. Therefore, the EDPB and EDPS recommend to include in the text of the Proposal that a DPIA must be performed by public sector bodies in case of data processing falling under Article 35 of the GDPR[43]. The DPIA will help to identify the risks and the appropriate data protection safeguards for the re-use addressing

[41] See Court of Justice of the European Union, C-201/14, *Smaranda Bara and Others*, 1 October 2015, ECLI:EU:C:2015:638.
[42] See Recital 14 of the Proposal
[43] See in this regard recital (53) of the Open Data Directive.

those risks, in particular for specific sectors routinely dealing with special categories of personal data. The decision on the re-use, in addition to being grounded on Union or Member State law, especially for some "sensitive sectors" (health sector, but also transport or energy grids) should be based on this assessment, as well as the specific conditions for the re-users and the concrete safeguards for data subjects(for example, clarifying the risks of re-identification of anonymised data and the safeguards against those risks). Finally, the results of such assessment, whenever possible, should be made public, as a further measure enhancing trust and transparency[44].

89. As for the conditions for re-use, Article 5(3) of the Proposal specifies that public sector bodies "may" impose an obligation to re-use only prior anonymized or pseudonymised personal data. This means that public sector bodies are not obliged to pre-process personal data so that to make available to re-users only prior anonymized or pseudonymised personal data. Consequently, public sector bodies may disclose to re-users even data which allow the natural persons - to whom the data relate - to be directly identified, if provision of anonymised data "would not respond to the needs of the re-user" [45]. In this case, on-premise or remote re-use of personal data within a secure processing environment could still be permitted by public sector bodies under Article 5(4) of the Proposal. However, given the rapid developments in re-identification techniques and the availability of advanced computational resources, the legislator should take into account that anonymisation, pseudonymisation, and even the use of secure environments cannot be considered in all cases as free from vulnerabilities, especially in the long term.

90. In this context, the EDPB and the EDPS welcome that recital 11 of the Proposal envisages that "the use of such secure processing environment" may be made by the public sector body *"conditional on the signature by the re-user of a confidentiality agreement that prohibits the disclosure of any information that jeopardises the rights and interests of third parties that the re-user may have acquired despite the safeguards put in place"*. **However, the EDPB and the EDPS also recommend to include a reference to such confidentiality agreement in the legal text of the Proposal among the conditions for re-use laid down in Article 5. This agreement should also prohibit the re-users from re-identifying any individual to whom the data relates and should contain the obligation for the re-users to assess on an on-going basis the risks of re-identification and to report any data breach resulting in the re-identification of the individuals concerned not only to the Data Protection Authority and the data subjects pursuant to Articles 33 and 34 of the GDPR, but also to the public sector body concerned.**

91. **In any case, the EDPB and EDPS emphasize that anonymisation and pseudonymisation cannot be placed at the same level and should be weighted differently by public sector bodies in assessing the re-use from a data protection perspective. Indeed, anonymisation represents a means of fostering the public sector information re-use in a pro-competitive perspective, while also meeting the various requirements under data protection legislation, given that 'anonymous information', as defined in Recital 26 of the GDPR, does not fall within the scope of the said legislation. On the contrary, information which has undergone pseudonymisation (which could lead to re-identification by a natural person by the use of additional information) should still be considered "personal data", thus entailing the application of other measures required by the data protection legislation, while reducing the risks for data subjects and helping public sector bodies and re-users to meet data protection obligations (in particular the principles of data protection by design and by default and data minimisation). The latter considerations apply also to the measures envisaged by Article 5(4) of the Proposal that public sector bodies may impose as conditions for re-use.**

[44] See EDPS Opinion on the proposal for a recast of the Public Sector Information (PSI) re-use Directive, available at: https://edps.europa.eu/sites/edp/files/publication/18-07-11_psi_directive_opinion_en.pdf
[45] See recital 11 of the Proposal

3.3.3 Article 5(11): re-use of "highly sensitive" non-personal data

92. Article 5(11) introduces the concept of non-personal data that have been identified as "highly sensitive", as regards the transfer to third countries, by Union law. Recital 19 of the Proposal provides some examples: "in the health domain, certain datasets held by actors in the public health system, such as public hospitals" "identified as highly sensitive health data", "for example in the context of the European Health Data Space or other sectoral legislation". With regard to such non-personal data, the Commission shall adopt delegated acts laying down special conditions applicable to the transfer of such data to third countries.

93. In this regard, the EDPB and the EDPS note that even if information in a anonymised data set does not present a risk of directly identifying or singling out a natural person, when this information is combined with other available information, it could entail the risk of indirect identification, so that it is likely to fall within the scope of the definition of personal data. Indeed, the more information is available and data are re-used and shared, the more difficult it will be to ensure anonymisation over time.[46] Consequently, the EDPS and the EDPB would like to draw attention to the fact that much of the data already today -and increasingly in the future- generated and processed by techniques of artificial intelligence, machine learning, internet of things, cloud computing and big data analysis, are often likely to fall within the scope of the definition of personal data. In this scenario, **the EDPB and the EDPS calls upon the legislator to consider that even the re-use of non-personal "highly sensitive" data envisaged by the Proposal may have an impact on the protection of personal data, especially if such non-personal data are the result of the anonymisation of personal data and thus information originally related to individuals.** Indeed also in these cases, the data subjects' fundamental rights to privacy and data protection must be fully ensured. Moreover, the EDPB and the EDPS strongly recommend clarifying the concept of "highly sensitive non-personal data", as a minimum by providing concrete examples.

3.3.4 Article 6: fees for data re-use

94. As for the fees envisaged under Article 6 of the Proposal, the EDPB and the EDPS note that the Open Data Directive contains an explicit reference to 'anonymisation costs' in Recitals 36 and 38 as well as in Article 6, paragraphs (1), (4) and (5). In particular, the Open Data Directive provides for an exception to the re-use of documents free of charge in order to allow public sector bodies to charge re-users the reasonable expenses they incur in to pre-process, aggregate and/or anonymise the personal data

[46] See in this regard, the WP29 Opinion 05/2014 on Anonymisation techniques (WP 216) as well as the Judgment of the ECJ of 19 October 2016, Patrick Breyer v Bundesrepublik Deutschland, in case C-582/14 which refers to Recital 26 of Directive 95/46/EC, looking at the legal and practical means by which re-identification may be affected by the use of additional data in the hands of third parties. The forthcoming EDPB guidelines on anonymisation/pseudonymisation will further elaborate upon this matter.

offered for re-use, in situations where the use of such techniques would be justified in light of the increased risks deriving from offering such data for re-use.

95. Given that, in certain cases, the pseudonymisation or anonymisation of information held by public sector bodies can be a complex, time-consuming and expensive task requiring expertise that might not always be available, the EDPB and the EDPS recommend including in Article 6(5) of the Proposal that **fees charged by public sector bodies for allowing the re-use of data may duly take into account the costs incurred by public sector bodies for the pseudonymisation or anonymisation** of personal data made available for reuse.

96. It can also be noted that **the Proposal reverses the general principle established by the Open Data Directive of "free of charge" re-use.** Indeed, Article 6(1) of the Proposal states that "*public sector bodies which allow re-use of the categories of data referred to in Article 3 (1) may charge fees for allowing the re-use of such data.*" In this regard, the interplay with the Open Data Directive is therefore unclear.

97. Moreover, it can be observed that, even though Article 6(5) specifies that "Fees shall be derived from the costs related to the processing of the requests for re-use (…)", the Proposal seems to introduce financial incentives to public sector bodies to allow the re-use of personal data.

98. It also has to be noted thatArticle 6(4) imposes an obligation to public sector bodies to "*take measures to incentivize the reuse of the categories of data referred to in Article 3 (1) [which include personal data] for non-commercial purposes and by small and medium-sized enterprises in line with State aid rules*."

99. This aspect, also in the light of the criticalities of the Proposal described in the general comments of this Joint Opinion, is problematic from a data protection viewpoint, under both legal and practical implementation's perspective. In particular, the lack of clarity on the type of incentives and addressees thereof may raise additional questions as to whether consent, as one of the legal basis relied upon under Article 5(6) of the Proposal for the re-use personal data, will be the appropriate legal ground, especially with regard to the individuals' freedom of choice to refuse to provide their consent to the re-use of their personal data or to withdraw it[47].

3.3.5 Governance and institutional aspects: Article 7 (competent bodies). Article 8 (single information point).

100. The Proposal provides that Members States will have to set up a single contact point for reuse of public sector data (Article 8), and to establish bodies in charge of supporting public sector bodies with technical means and legal assistance for reuse of public sector data (Article 7). Pursuant to Article 7(3), such "competent bodies" may be entrusted to grant access for the reuse of data, including personal data.

[47] As stated in the EDPB Guidelines 05/2020 on consent under GDPR, in general terms, any element of inappropriate pressure or influence upon the data subject (which may be manifested in many different ways) which prevents a data subject from exercising their free will, shall render the consent invalid.

101. Therefore, with regard to the competent bodies, they will, inter alia, assist the public sector bodies in obtaining consent or permission for the re-use and can also be entrusted to grant access for the re-use of data held by the public sector body, including personal data.

102. Firstly, the provision under Article 7(2)(c) should be clarified, due in particular to the vagueness of the terminology used ("permission by re-users for reuse"; "altruistic and other purposes"; "in line with specific decisions of data holders"). The overall meaning of the provision ("the competent bodies assist the public sector bodies, where relevant, in obtaining consent or permission *by re-users for re-use* for altruistic and other purposes in line with specific decisions of data holders") is therefore also unclear.

103. Secondly, despite those bodies are essentially tasked with support and advisory duties vis-à-vis public sector bodies for data re-use, some of their tasks deal with implementing the safeguards set out in the data protection legislation and fostering the protection of the rights and interests of individuals with regards to their personal data. However, Chapter II of the Proposal does not clarify whether data protection supervisory authorities - to which the GDPR also confers, among others, advisory powers - may be designated as the competent body under Article 7 of the Proposal[48].

104. In this regard, the EDPS and the EDPB firstly underline that the designation and multiplication of competent bodies that may deal, to some extent, with personal data processing under Chapter II of the Proposal could lead to real complexity for public sector bodies, re-users and data subjects, and also affect consistency in terms of monitoring the application of the provisions of the GDPR. **Hence, inasmuch as personal data is being subject to re-use on the basis of the Proposal, the EDPB and the EDPS consider that the data protection supervisory authorities should be the only ones competent for the oversight of such personal data processing. Adequate resources should be provided to these authorities to allow them to effectively and efficiently perform this task.**

105. **Furthermore, should specific bodies be designated to assist public sector bodies and data re-users and be entrusted to grant access for the reuse of data, including personal data, such bodies may not be referred as "competent" as they would not act as a supervisory authority able to monitor and enforce the provisions related to the processing of personal data. In order to ensure legal certainty and consistency of the application of the EU acquis in the field of personal data protection, the activities and obligations of such designated bodies shall also be subject to the direct competence and supervision of data protection authorities, when personal data is involved.**

106. **As per their competence and tasks under the GDPR, data protection authorities have already specific expertise in the monitoring of the compliance of data processing, as well as in promoting awareness of controller and processor of their obligation related to the processing of personal data. Therefore, in order to ensure consistency between the institutional framework envisaged by Chapter II of the Proposal and the GDPR, the EDPB and the EDPS recommend to clarify that the main competent authorities for the supervision and enforcement of the provisions of Chapter II related to the processing of personal are the data protection supervisory authorities. The latter authorities should**

[48] As it is the case, for example, in the context of existing data spaces, such as the French Health Data Hub, where the FR data protection authority is the one competent to authorise access to specific personal data. See also in this regard the advisory powers conferred to the data protection authorities in the context of a DPIA, in order ensure their compliance with the rules for the protection of personal data according to Articles 57(1)(l) and 58(3)(a) of the GDPR.

work closely with the specific bodies designated, under the Proposal, to assist public sector bodies and re-users and entrusted to grant access for the reuse of data, in consultation with other relevant sectorial authorities, when necessary, so as to ensure a coherent application of these provisions.

107. The EDPB and the EDPS also observe that the Proposal does envisage under Article 8(4) a mechanism for redress for re-users where they wish to challenge the decision of refusing access for re-use that is different from the one established under the Open Data Directive. Under the Open Data Directive (See Article 4(4)), in particular, the means of redress shall include the possibility of review by an impartial review body with the appropriate expertise, such as, among others, *"the supervisory authority established in accordance with Regulation (EU) 2016/679 or a national judicial authority, whose decisions are binding upon the public sector body concerned"*. In this respect, without prejudice to the observations already made in this Joint Opinion on the need of clarifying the interplay of the Proposal with the Open Data Directive, the EDPB and the EDPS call the attention of the legislator on the inconsistencies between those two set of rules.

3.4 Requirements applicable to data sharing service providers

The Explanatory Memorandum illustrates that "*Chapter III aims to increase trust in sharing personal and non-personal data and lower transaction costs linked to B2B and C2B data sharing by creating a notification regime for data sharing providers. These providers will have to comply with a number of requirements, in particular the requirement to remain neutral as regards the data exchanged. They cannot use such data for other purposes. In the case of providers of data sharing services offering services for natural persons, the additional criterion of assuming fiduciary duties towards the individuals using them will also have to be met. The approach is designed to ensure that data sharing services function in an open and collaborative manner, while empowering natural and legal persons by giving them a better overview of and control over their data. A competent authority designated by the Member States will be responsible for monitoring compliance with the requirements attached to the provision of such services*."[49]

108. Article 9(1) of the Proposal, specified under recital 22, sets out three different types of data sharing services:

- under letter (a), intermediary between data holders which are legal persons and potential data users;

- under letter (b), intermediation services between data subjects and potential data users;

- under letter (c), 'data cooperatives'.

109. Having regard to the first type of data sharing service, Article 9(1)(a) refers to "*intermediation services between data holders which are legal persons and potential data users, including making available the technical or other means to enable such services; those services may include bilateral or multilateral exchanges of data or the creation of platforms or databases enabling the exchange or joint exploitation of data, as well as the establishment of a specific infrastructure for the interconnection of data holders and data users.*"

[49] Explanatory Memorandum, page 7.

110. Recital (22) specifies: "*Providers of data sharing services (data intermediaries) are expected to play a key role in the data economy, as a tool to facilitate the aggregation and exchange of substantial amounts of relevant data. Data intermediaries offering services that connect the different actors have the potential to contribute to the efficient pooling of data as well as to the facilitation of bilateral data sharing. Specialised data intermediaries that are independent from both data holders and data users can have a facilitating role in the emergence of new data-driven ecosystems independent from any player with a significant degree of market power. This Regulation should only cover providers of data sharing services that have as a main objective the establishment of a business, a legal and potentially also technical relation between data holders, including data subjects, on the one hand, and potential users on the other hand, and assist both parties in a transaction of data assets between the two. It should only cover services aiming at intermediating between an indefinite number of data holders and data users, excluding data sharing services that are meant to be used by a closed group of data holders and users.*"

111. **In light of the above, the EDPB and the EDPS consider that the issue referred to under the general remarks of this Joint Opinion as overarching concern, namely the risk that the Proposal creates a parallel set of rules, which are not consistent with the GDPR, is particularly evident with reference to Chapter III of the Proposal. Indeed, it is unclear the interplay of the provisions under Article 9 of the Proposal, referring to 'data holders', 'potential data users', 'the exchange or joint exploitation of data', 'the interconnection of data holders and data users', with the rules and principles of the GDPR.**

112. We recall that the data sharing service as platform "intermediating between an indefinite number of data holders and data users" excluding the use by a closed group of data users, in so far as the intermediation relates to personal data, shall be compliant in particular with the principle of data protection by design and by default under Article 25 of the GDPR[50].

[50] See Article 25(2): "The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data **are not made accessible without the individual's intervention to an indefinite number of natural persons**."
See also EDPB Guidelines 4/2019 on the principle of privacy by design and by default, at page 20:
"Key design and default purpose limitation elements may include:
- Predetermination – The legitimate purposes shall be determined before the design of the processing.
- Specificity – The purposes shall be specified and explicit as to why personal data is being processed.
- Purpose orientation – The purpose of processing should guide the design of the processing and set processing boundaries.
- Necessity – The purpose determines what personal data is necessary for the processing.
- Compatibility – Any new purpose must be compatible with the original purpose for which the data was collected and guide relevant changes in design.
- Limit further processing – The controller should not connect datasets or perform any further processing for new incompatible purposes.
- Limitations of reuse – The controller should use technical measures, including hashing and encryption, to limit the possibility of repurposing personal data. The controller should also have organisational measures, such as policies and contractual obligations, which limit reuse of personal data.

113. The EDPB and the EDPS also point out to the data protection principles of transparency (and purpose limitation) of the processing of personal data. As stated in the WP29 Guidelines on transparency "*the data subject should … be able to determine in advance what the scope and consequences of the processing entails*" (…) "*namely the kind of effect will the specific processing described in a privacy statement/notice actually have on a data subject*".[51]

114. **The concept of data sharing service as platform "intermediating between an indefinite number of data holders and data users", as kind of open data marketplace, would be contrary to the aforesaid data protection principles of privacy by design and by default, transparency and purpose limitation if the platform does not allow a pre-selection of and prior information about the purposes and users of her or his personal data by and to the data subject. For the sake of clarity, the Proposal should specify, at least in a recital, this aspect.**

115. **The scope of the notion of data intermediary between data holders and legal persons is also unclear, and hence should be better specified**[52].

116. As a general observation, it can also be remarked that the Proposal does not specify **how (according to which GDPR legal basis) data sharing service providers will collect personal data for the sharing purposes.**

117. It is also unclear **whether data sharing service providers can intermediate data allowed for re-use by public sector bodies** under Chapter II of the Proposal.

118. It is also key, for transparency reasons and to increase (rather than decrease) the level of citizens' trust, to make clear in the Proposal that the data sharing service will be provided upon payment of a 'price' by data holders and data users. This aspect can be deducted from the wording of Article 11(3) of the Proposal[53], but is unclear and incomplete (it does not provide a clear picture of the monetary transactions accompanying the processing of personal data). The clear incentive to 'monetize' personal data also increases the importance of checks on data protection compliance[54]. Regrettably, in this regard, as well as in relation to the other chapters of the Proposal, the impact assessment[55] does not take the data protection risks into account.

119. Moreover, the EDPB and the EDPS observe that the Proposal does not provide a clear picture, for instance via examples in the recitals, of the 'use cases' of data sharing services (whose 'monetary transaction aspect', as highlighted, shall be made clear to the public and to the persons concerned when this is the case). For instance, recital (22) specifies what is not a data exchange platform to be considered 'data intermediary': "*Data exchange platforms that are exclusively used by one data holder in order to enable the use of data they hold as well as platforms developed in the context of objects and devices connected to the Internet-of-Things that have as their main objective to ensure functionalities of the connected object or device and allow value added services, should not be covered by this Regulation*", but does not provide in this regard the envisaged use case.

3.4.1 Data intermediaries under Article 9(1) (b): intermediation services between data subjects and potential data users[56].

120. The EDPB and the EDPS note that the provisions related to intermediation services between data subjects that seek to make their personal data available and potential data users in the exercise of the rights provided in Regulation (EU) 2016/679, as per article 9(1)(b), is to be applied without prejudice to the effective application of the data subjects' rights and data controller's obligations as per the GDPR.

121. The Proposal however does not specify the modalities upon which such service providers would effectively assist individuals in exercising their rights under the GDPR nor provides indication as to which personal data processing such assistance would apply and towards which data users precisely[57].

122. The EDPB and the EDPS first of all consider that the effective exercise of data subjects' rights and the possible modalities for such exercise are provided for by the GDPR, under the monitoring of national supervisory authorities as per Article 51 of that same Regulation. The lack of clarity on the precise

- Review – The controller should regularly review whether the processing is necessary for the purposes for which the data was collected and test the design against purpose limitation."

[51] EDPB Guidelines on transparency under Regulation 2016/679 WP260, rev.01, page 7.

[52] Recital 22 specifies: "[..] Providers of **cloud services** should be excluded, as well as **service providers that obtain data from data holders, aggregate, enrich or transform the data and licence the use** of the resulting data to data users, without establishing a direct relationship between data holders and data users, for example **advertisement or data brokers, data consultancies, providers of data products resulting from value added** to the data by the service provider. At the same time, data sharing service providers should be allowed to make **adaptations to the data exchanged, to the extent that this improves the usability** of the data by the data user, where the data user desires this, such as to convert it into specific formats. In addition, **services that focus on the intermediation of content, in particular on copyright-protected content, should not be covered** by this Regulation.
Data exchange platforms that are exclusively used by one data holder in order to enable the use of data they hold as well as platforms developed in the context of objects and devices connected to the Internet-of-Things that have as their main objective to ensure functionalities of the connected object or device and allow value added services, should not be covered by this Regulation. 'Consolidated tape providers' in the sense of Article 4 (1) point 53 of Directive 2014/65/EU of the European Parliament and of the Council as well as 'account information service providers' in the sense of Article 4 point 19 of Directive (EU) 2015/2366 of the European Parliament and of the Council should not be considered as data sharing service providers for the purposes of this Regulation. Entities which restrict their activities to facilitating use of data made available on the basis of data altruism and that operate on a not-for-profit basis should not be covered by Chapter III of this Regulation, as this activity serves objectives of general interest by increasing the volume of data available for such purposes."

[53] Article 11(3) of the Proposal lays down: "the provider shall ensure that the procedure for access to its service is fair, transparent and non-discriminatory for both data holders and data users, including as regards **prices**."

[54] In this regard, the EDPB is developing guidance on the collection and use of personal data against financial remuneration.

[55] Impact Assessment accompanying the Data Governance Act, SWD(2020) 295 final, available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SWD:2020:0295:FIN:EN:PDF

[56] Article 9(2)(b) of the Proposal refers to: "intermediation services between data subjects that seek to make their personal data available and potential data users, including making available the technical or other means to enable such services, in the exercise of the rights provided in Regulation (EU) 2016/679."

[57] Article 11(10) of the Proposal is still quite vague in its wording "the provider offering services to data subjects **shall act in the data subjects' best interest when facilitating the exercise of their rights**, in particular by advising data subjects on potential data uses and standard terms and conditions attached to such uses;"

modalities in the assistance provided for the exercise of data subjects' rights, as well as on the recipients of such process and their obligations towards data subjects may lead to further legal uncertainties in effectively exercising data subjects' rights as per the GDPR.

123. **The EDPB and the EDPS would therefore recommend that the Proposal reflects the EU legal framework (GDPR) according to which such modalities, as well as related obligations applicable to data sharing services providers and recipients, can be further specified by the European Data Protection Board, in accordance with Article 70 of the GDPR[58].**

124. It is also unclear whether the intermediation services under letter (b) of Article 9(1) of the Proposal, for which a definition is not provided under its Article 2, refer to and refer only to (and to which extent) Personal Information Management Systems (PIMS). The EDPB and the EDPS point out to the difference between PIMS, allowing management of personal data and facilitating the exercise of data subjects' rights ('interfacing with the data subject')[59], on the one hand, and business to business data sharing service providers (whose correlation with 'data brokers' is unclear), on the other hand. It is in relation to the latter, where the data subject is more far-way and at risk of not having a clear overview and control over the sharing of his or her personal data, that criticalities under the data protection viewpoint may be higher[60].

125. However, in all cases transparency, fairness and purpose limitation principles shall apply.

126. In its Opinion on PIMS, the EDPS pointed out that *"In any event, it is crucial to ensure the transparency of the business model vis-à-vis the individuals whose data are being processed so that they are aware of the interests at stake (of PIMS and other service providers) and can use PIMS in full awareness"* [61].

[58] In this regard, the EDPB is currently working on guidelines on data subject rights.
[59] See the EDPS Opinion on Personal Information Management Systems, 20 October 2016, available at: https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_en.pdf
[60] See EDPS Opinion on the European Strategy for Data, paragraph 20: "At the same time, the EDPS underlines the need of caution with regard to the role of data brokers that are actively engaged in the collection of huge datasets, including personal data from different sources. They tap into a variety of data sources used for data-related services, such as data that are disclosed for other unrelated purposes; data from public registers (open data), as well as data "crawled" from the Internet and social media, often in violation of data protection legislation. In this context, the EDPS notes that the activities of big data brokers are under increased scrutiny and are investigated by a number of national data protection authorities."
[61] See page 13, para. 52, of the EDPS Opinion on Personal Information Management Systems, 20 October 2016, available at: https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_en.pdf
See also para 53, page 13: "*The model of PIMS seems to invite a debate over who 'owns' our personal data. Individuals in the EU have a fundamental right to the protection of their personal data, based upon Article 8 of the EU Charter of Fundamental Rights. Detailed rights and obligations relating to the exercise of this right are regulated in further detail in the recently adopted GDPR. These issues are not specific to PIMS: personal data is often perceived as the 'currency' we pay for so-called 'free' services on the internet. This trend does not, however, mean that personal data of individuals can legally be considered as property which can be traded freely as any other property on the market. On the contrary, as a matter of principle PIMS will not be in a position to 'sell' personal data, but rather, their role will be to allow third parties to use personal data, for* ***specific purposes****, and* ***specifics periods of time****, subject to* ***terms and conditions identified by the individuals themselves****, and* ***all other safeguards provided by applicable data protection law****.*"

127. The Proposal provides some clarifications related to providers of data sharing services not established in the Union in order to determine whether such a provider is offering services within the Union. This specification, under recital 27 of the Proposal, seems in line with recital (23) of the GDPR. It might be useful, for the sake of legal certainty, specifying that, in case of processing of personal data, the aforesaid data sharing service providers not established in the Union are subject to the rules and principles of the GDPR.

3.4.2 Data intermediaries under Article 9(1) (c): 'data cooperatives'

128. The EDPB and the EDPS underline that the notion of "service of data cooperatives", introduced in Article 9(1)(c) of the Proposal[62], remains unclear both in terms of nature and obligations. In this regard, a clear definition of such data sharing services providers, as well as their applicable obligations, should be introduced in order to avoid any legal uncertainty in the provision of such services.

129. While the Proposal specifies that data cooperatives "*seek to strengthen the position of individuals in making informed choices before consenting to data use, influencing the terms and conditions of data user organisations attached to data use or potentially solving disputes between members of a group on how data can be used when such data pertain to several data subjects within that group*"[63], it is to be recalled that transparency obligations, as well as the conditions for the valid consent of the data subject as per Article 6(1)(a) of Regulation (EU) 2016/679 and the condition for the processing of personal data under this legal basis, are defined and provided for by that same regulation.

130. **The EDPB and the EDPS therefore consider that the position of individuals in making informed choice, or the solving of potential dispute on how data can be used, are not to be considered as negotiable conditions but rather as data controllers' obligations as per Regulation (EU) 2016/679. In this regard, it is also to be pointed out that the reference in Recital (24) of the Proposal to data that would "pertain" to several data subject, insofar as it relates to personal data, may not be consistent with the definition of personal data as per Regulation (EU) 2016/679[64], which refers to "any information relating to an identified or identifiable natural person".**

131. Furthermore, as recalled in Recital (24) of the Proposal, "*the rights under Regulation (EU) 2016/679 can only be exercised by each individual and cannot be conferred or delegated to a data cooperative*". The EDPB and the EDPS consider that the articulation of such principles with the possibility for data cooperatives to be conferred powers to "negotiate terms and conditions for data processing before they consent" is unclear at least, if not directly contradictory. Indeed, the "terms and conditions" for the processing of personal data are - as a matter of fact - those enshrined in the GDPR and, therefore, they cannot be amended or superseded by means of a contract or other type of private arrangements.

[62] Article 9(2)(c) of the Proposal refers to "services of data cooperatives, that is to say services supporting data subjects or one-person companies or micro, small and medium-sized enterprises, who are members of the cooperative or **who confer the power to the cooperative to negotiate terms and conditions for data processing before they consent**, in **making informed choices before consenting to data processing**, and **allowing for mechanisms to exchange views on data processing purposes and conditions that would best represent the interests of data subjects or legal persons**."
[63] Recital (24) of the Proposal.
[64] Definition under Article 4(1) of the GDPR.

3.4.3 Article 10: notification regime - general requirements to be eligible for registration - content of the notification; outcome (and timing) of the notification. Article 11: conditions for providing data sharing services

132. Chapter III of the Proposal establishes an obligation for providers of data sharing services as described under Article 9(1) to submit a notification to the competent authority (mandatory notification). Article 10(1) and (2) provide rules on the identification of the jurisdiction of the Member State for the purposes of the Proposal. This is the jurisdiction of the Member State of the main establishment of the data sharing service provider or the Member State of establishment of the legal representative of the data sharing service provider not established in the Union.

133. The information to be included in the notification is provided under Article 10(6), letters (a)-(h) of the Proposal[65]. In addition, Article 10(7) lays down that "*At the request of the provider, the competent authority shall, within one week, issue a standardised declaration, confirming that the provider has submitted the notification referred to in paragraph 4.*"

134. The notification regime, as highlighted in the Explanatory Memorandum, "consists of a *notification obligation with ex post monitoring of compliance with the requirements to exercise the activities by the competent authorities of the Member States*"[66]. This aspect is further specified under recitals (30) and (31) of the Proposal[67].

135. Hence, the 'vetting' of the data sharing service provider is limited to the verification by the competent authority of the (mainly formal) requirements set out in Article 10 and shall occur within a very short time-limit (one week from the date of notification).

[65] "The notification shall include the following information:
(a) the name of the provider of data sharing services;
(b) the provider's legal status, form and registration number, where the provider is registered in trade or in another similar public register;
(c) the address of the provider's main establishment in the Union, if any, and, where applicable, any secondary branch in another Member State or that of the legal representative designated pursuant to paragraph 3;
(d) a website where information on the provider and the activities can be found, where applicable;
(e) the provider's contact persons and contact details;
(f) a description of the service the provider intends to provide;
(g) the estimated date for starting the activity;
(h) the Member States where the provider intends to provide services."

[66] Explanatory Memorandum, page 5.

[67] "(30) A notification procedure for data sharing services should be established in order to ensure a data governance within the Union based on trustworthy exchange of data. The benefits of a trustworthy environment would be best achieved by imposing a number of requirements for the provision of data sharing services, but **without requiring any explicit decision or administrative act by the competent authority for the provision of such services**.
(31) In order to support effective cross-border provision of services, the data sharing provider should be requested to **send a notification only to the designated competent authority from the Member State where its main establishment is located or where its legal representative is located**. Such a **notification should not entail more than a mere declaration of the intention to provide such services and should be completed only by the information set out in this Regulation**." (emphasis added)

136. **In this regard, the EDPB and the EDPS note that the 'vetting' regime is almost 'declarative' and that the Commission has opted for the most 'loose' regime (as opposed for instance to an authorization regime). The EDPB and the EDPS observe that, at least with regard to the processing of personal data, the regime should be more protective (that is, provide more checks and safeguards for the data subjects, including on the crucially important data protection aspects). This would also allow ensuring the higher level of trust aimed at by the Commission.**

137. **In order to address this concern, in particular Recital 31 of the Proposal should be amended.**

138. According to the data protection principle of accountability, data sharing service providers shall be able among others to demonstrate that they put in place policies and procedures that allow data subjects to easily exercise their individual data protection rights (procedures for ensuring compliance with data subjects' rights), and should document the decisions about the data sharing (including in particular the purposes for which the personal data will be shared and the recipients or categories of recipients to whom they will be disclosed), evidencing their compliance with data protection law[68]. These aspects (which should form the 'core' of the labelling envisaged by the Proposal[69]) will have the effect of creating greater trust in data sharing service providers by the public.

139. The EDPB and the EDPS also remark that the provisions of data sharing services, as laid down under Article 11, shall be subject to conditions under (1)-(11). In this regard, the EDPB and the EDPS notice that while reference is made among the conditions to compliance with competition rules (under (9)), these (exhaustively listed) conditions do not include compliance with data protection rules.

140. **In light of the elements above, and considering the possible risk for data subject in the personal data processing that may be undertaken by data sharing service providers, the EDPB and the EDPS consider that the declaratory notification regime as laid down in the Proposal does not provide for a sufficiently stringent vetting procedure applicable to such services. The EDPB and the EDPS recommend exploring alternative procedures which should notably take into account a more systematic inclusion of accountability and compliance tools for the processing of personal data as per the GDPR, in particular the adherence to a code of conduct or certification mechanism.**

[68] According to Article 30 of the GDPR: "Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information: (a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer; (b) the purposes of the processing; (c) a description of the categories of data subjects and of the categories of personal data; (d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations; (e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards; (f) where possible, the envisaged time limits for erasure of the different categories of data; (g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1). [...]"

[69] The Impact Assessment of the Proposal refers to labelling or certification, among others, at page 19 "Mutual recognition of certification/labelling mechanisms and of a trust scheme for data altruism will make it possible to collect and use the data at the necessary scale."; page 25 "certification/labelling framework for data intermediaries"; page 26: "A certification or labelling framework would allow novel data intermediaries to increase their visibility as trustworthy organisers/orchestrators of data sharing or pooling."

141. It can also be observed that the safeguards provided in Chapter IV of the Proposal for data altruism organizations (Article 18, transparency requirements; Article 19, specific requirements) are not foreseen by the Proposal having regard to data sharing service providers, despite the possible impact also of these data sharing services on the rights and freedoms of the persons concerned.

142. This difference between the two notification regimes might give raise to interpretation *a contrario* that the requirements established for data altruism organizations and relating to the protection of personal data insofar as personal data are processed (for instance, informing data holders about any processing outside the Union[70]) do not apply to data sharing service providers.

143. **In this regard, the EDPB and the EDPS notice in particular that organisations involved in 'data pooling' or data sharing arrangements should adhere to certain common standards, whose supervision by independent data protection authorities shall be expressly recalled by the Proposal, related not only to the conditions for interoperability, but also to the conditions for ensuring the lawfulness of the processing of personal data and facilitating the exercise of data subject rights (e.g., through joint controllers' arrangements pursuant to Article 26 of the GDPR).**

144. Moreover, the EDPB and the EDPS notice that the Proposal refers to scenarios (use of metadata for the development of the data sharing service, under Article 11(2); continued access by data holders and data users after insolvency of the data sharing provider to data stored by the latter, under Article 11(6)) which need specifications in order to bring them in line with rules and principles on the protection of personal data.

145. The EDPB and the EDPS also remark that the comments made under the general remarks of this opinion, related to the definitions used in the Proposal and to the issue of the legal basis under the GDPR for the processing of personal data, are also relevant having regard to the provisions of Chapter III of the Proposal.

146. Furthermore, with particular reference to the aim of ensuring better control on the access and use of personal data by the data subject, we recall that the principle of purpose limitation is of special importance having regard to business-to-business data intermediaries. Recital (26) of the Proposal[71], which seems to identify the purpose of the processing of personal data with the intermediation in the sharing of data, without further specifications, might raise concerns from a data protection viewpoint[72].

[70] Article 19(1)(b) of the Proposal.

[71] Recital (26) of the Proposal: "A key element to bring trust and more control for data holder and data users in data sharing services is the neutrality of data sharing service providers as regards the data exchanged between data holders and data users. It is therefore necessary that data sharing service providers **act only as intermediaries** in the transactions, and do not use the data exchanged for **any other purpose**. [..]"

[72] See also Article 2(4) of the Proposal: 'metadata' means data collected on any activity of a natural or legal person **for the purposes of the provision of a data sharing service"**; Article 2(7): "'data sharing' means the provision by a data holder of data to a data user for **the purpose of joint or individual use of the shared data**"; Article 11(1): the provider may not use the data for which it provides services for **other purposes than to put them at the disposal of data users.**"

147. The EDPB and the EDPS consider that the remarks made under Section 3.3 of this Joint Opinion concerning the reuse of personal data held by public sector bodies are also relevant having regard to data sharing services:

- any sharing or access to personal data must be strictly defined in scope and purpose and must occur in full compliance with the GDPR, taking into account the requirements of lawfulness, purpose limitation and the legitimate expectations of the data subjects;

- it should be clear that each 'actor' of the data processing chain, including the data sharing service provider and the user(s), shall provide the data subjects with the information under Article 13 and 14 of the GDPR (oftentimes, Article 14, applicable where personal data have not been obtained by the data subject, will be the relevant provision of the GDPR in this context). We recommend adding in this regard that the data sharing service provider shall provide the data subject with user-friendly tools showing him/her a comprehensive view of how his/her personal data are shared, as well as a user-friendly tool to withdraw consent in case the service provided consists of a tool for obtaining consent from data subjects with regard to the processing of their personal data under Article 11(11) of the Proposal

- the data protection impact assessment (DPIA) is a key tool to ensure that data protection requirements are properly taken into account and the rights and interests of individuals are adequately protected, so as to foster their trust in the re-use mechanism. Therefore, the EDPB and EDPS recommends to include in the text of the Proposal that **a DPIA must be performed by data sharing service providers (and by the data user) in case of data processing falling under Article 35 of the GDPR**. Indeed, the data sharing envisaged under the Proposal may involve large-scale processing, which combines data from a variety of sources, potentially involving special categories of data and/or personal data of vulnerable groups of data subjects. In this case, data controllers have the obligation to perform a DPIA in accordance with Article 35 of the GDPR. Moreover, whenever possible, the results of such assessments, as a trust and transparency-enhancing measure, shall be made public by the data sharing service provider as well as by the user(s).

3.4.4 Articles 12 and 13: competent authorities and monitoring of compliance (with Articles 10 and 11).

148. Article 12(3) of the Proposal provides that "*The designated competent authorities, the data protection authorities, the national competition authorities, the authorities in charge of cybersecurity, and other relevant sectorial authorities shall exchange the information which is necessary for the exercise of their tasks in relation to data sharing providers.*"

149. This wording provides for an even minor role for data protection authorities than the wording used by the Proposal in relation to data altruism organisations[73], which refers to "*cooperation with data protection authorities*".

[73] Article 20(3): "The competent authority shall undertake its tasks [of authority responsible for the register of recognised **data altruism organizations** and for the monitoring of compliance with the requirements of Chapter

150. In this regard, as highlighted in Section 3.7 of this Joint Opinion, the EDPB and the EDPS recall that many provisions of this Chapter as well as of the other Chapters of the Proposal relate to the processing of personal data and that the data protection authorities are the authorities 'constitutionally' competent for the supervision related to the protection of personal data pursuant to Article 8 of the Charter and Article 16 TFEU.

151. Having regard to Article 13 of the Proposal, monitoring of compliance, notwithstanding recital (24) *"the provisions of this Regulation are without prejudice to the responsibility of supervisory authorities under the GDPR"*, the EDPB and the EDPS consider that the governance and monitoring of compliance should be better defined in order to ensure a more appropriate vetting of data sharing service providers (and data altruism organisations) including on compliance with the GDPR; and to avoid, at the same time, any overlap or conflict of attribution between the authorities established under the Proposal (which, according to the wording of Articles 12(3) -and 20(3)-, are not data protection authorities) and the data protection authorities.

152. **The EDPB and EDPS therefore consider that such better definition of governance would be provided by the designation of data protection authorities as the main competent authorities to monitor and supervise compliance with the provisions of Chapter III of the Proposal.**

153. The designation of data protection authorities as the main competent authorities for the supervision and enforcement of the provisions under Chapter III of the Proposal would also ensure a more consistent regulatory approach across Member State and therefore contribute to the consistent application of the Proposal. As per their competence and tasks under the GDPR, data protection authorities have already specific expertise in the monitoring of the compliance of data processing, the auditing of specific data processing activities and data sharing, the assessment of the adequate measures to ensure a high level of security for the storage and transmission of personal data, as well as in promoting awareness among controllers and processors of their obligation related to the processing of personal data.

154. The designation of data protection authorities as main competent authority for the supervision and enforcement of the provisions under Chapter III shall be supported with the foreseen provision under Article 12(3) allowing for the exchange of information between the data protection authorities, the national competition authorities, the authorities in charge of cybersecurity, and other relevant sectorial authorities in order to ensure a coherent application of these provisions.

IV of the Proposal] **in cooperation with the data protection authority**, where such tasks are related to processing of personal data, and with relevant sectoral bodies of the same Member State. For any **question requiring an assessment of compliance with Regulation (EU) 2016/679**, the competent authority shall first seek an opinion or decision by the competent supervisory authority established pursuant to that Regulation and comply with that opinion or decision."
It also has to be noted that recital 28 -having regard to **providers of data sharing services**- specifies that "this Regulation should be **without prejudice to** the obligation of providers of data sharing services to comply with Regulation (EU) 2016/679 and **the responsibility of supervisory authorities to ensure compliance with that Regulation**." The same specification is **not** made having regard to data altruism organizations.

155. In addition, the EDPB and EDPS consider that, when monitoring compliance, the power of the competent authorities cannot be limited to "the power to request information", as it appears from Article 13(2) of the Proposal. This limitation definitely stems from the declaratory nature of the "labelling regime" envisaged by the Proposal, albeit it is not adequate to the level of vetting the labelling requires, due to the high expectations of data protection compliance resulting from such labelling, especially vis-à-vis data subjects.

156. Finally, the EDPB and EDPS emphasise that adequate resources should be provided to the data protection authorities in order to allow them to effectively and efficiently perform the necessary supervision.

3.5 Data altruism

3.5.1 Interplay between data altruism and consent under the GDPR

157. The concept of "data altruism" referred to in the Proposal covers situations where natural or legal persons make data voluntarily available for reuse, without compensation, for "*purposes of general interest, such as scientific research purposes or improving public services*"[74].

158. It can be argued that the Proposal does not "create" but "formalizes/codifies" the possibility for data holders (defined as including data subjects by the Proposal) to make data available voluntarily, already envisaged in the GDPR. Indeed, a data subject can already consent to the processing of personal data relating to her or him for, among others, scientific research purposes.

159. Despite the definition provided under Article 2(10) of the Proposal ("'data altruism' means the consent by data subjects to process personal data pertaining to them, or permissions of other data holders to allow the use of their non-personal data without seeking a reward, for purposes of general interest, such as scientific research purposes or improving public services"), the concept of *"data altruism"* is still not clearly and sufficiently defined. In particular, it is unclear whether the consent envisaged in the Proposal corresponds to the notion of "consent" under the GDPR, including the conditions for the lawfulness of such consent. In addition, it is unclear the added value of 'data altruism', taking into account the already existing legal framework for consent under the GDPR, which provides for specific conditions for the validity of consent.

160. The GDPR and the Proposal concurrently apply in case of processing of personal data by data altruism organisations. The EDPB and EDPS support the objective of facilitating the processing of personal data for well-defined purpose(s) of general interest, still such aim shall be achieved in full compliance with the applicable data protection rules and principles. In particular, the EDPB and the EDPS underline that one of the main objectives of the GDPR is to ensure that the data subject keeps control over her or his personal data. In this context, the EDPB and EDPS underline that **all requirements related to the consent, as set in the GDPR, need to be fulfilled**.

161. The EDPB and the EDPS reiterate that **the fundamental right to the protection of personal data cannot in any case be 'waived' by the individual concerned**, be it through an 'act of altruism' related

[74] Article 2(10) of the Proposal.

to personal data. The data controller (the data altruism organisation) remains fully bound by the personal data rules and principles even when the data subject has given consent to the data altruism organisation for the processing of personal data relating to him or her for one or more specified purpose(s).

162. **In light of the above, the Proposal should specify in the substantive part that it refers to consent as defined under Article 4(11) of the GDPR and that, pursuant to Article 7(3), the data altruism organisation shall make as easy to withdraw consent as to provide it[75].**

163. The EDPB and the EDPS also stress the fact that data processed by the data altruism organisations may include special categories of personal data, e.g. data concerning health.

164. The EDPB and the EDPS also underline that, in line with the principle of data minimisation, where it is possible and adequate to the purpose, data should be processed in anonymised form.

165. The EDPB and the EDPS welcome that the Proposal specifies under Article 22(3) that where personal data is provided to the data altruism organisation, the consent form shall ensure that individuals are able to provide and withdraw consent, for a specific data processing operation, in line with the GDPR.

166. In this regard, the EDPB and the EDPS consider that the rules for withdrawal of consent, including its consequences, should be clear. It should be clear in particular how both the data altruism organisation and the data users comply with the requests for withdrawal, including by deleting the personal data in accordance with Article 17(1)(b) GDPR. The EDPB and the EDPS recall that, when taking decisions on 'data altruism', data protection impact assessments may have to be performed by data altruism organizations in accordance with Article 35 of the GDPR.

167. Scientific research often involves the processing and sharing of special categories of personal data on a large scale and thus, in certain cases, the latter could be considered a high-risk data processing according to the GDPR. Furthermore, data protection impact assessments in this context should be conducted with the involvement of the data protection officer (DPO) and of an ethical review board and, where possible and as a matter of good practice, should be made public, or a summary thereof.

168. According to the GDPR, consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement.

169. Recital 33 of the GDPR underlines that it is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects

[75] See EDPB Guidelines 5/2020 on consent, at paras 121-122:
"121. Article 6 sets the conditions for a lawful personal data processing and describes six lawful bases on which a controller can rely. The application of one of these six bases must be established prior to the processing activity and in relation to a specific purpose.
122. It is important to note here that **if a controller chooses to rely on consent for any part of the processing, they must be prepared to respect that choice and stop that part of the processing if an individual withdraws consent.** Sending out the message that data will be processed on the basis of consent, while actually some other lawful basis is relied on, would be fundamentally unfair to individuals."

should be allowed to give their consent to certain areas of scientific research when in compliance with recognised ethical standards for scientific research[76]. This is also reflected in recital (38) of the Proposal.

170. However, the EDPB and the EDPS underline that granting this kind of consent for purposes of general interest[77] as such (not strictly defined and referring to a possibly different and much broader scope than scientific research) is not allowed under the GDPR.

171. Indeed, the Proposal, in its recital 35 refers to "purposes of general interest" by providing (not a definition, but) a non-exhaustive list of examples, which includes applied and privately funded research and technological development and data analytics[78].

172. **In light of the above, the EDPB and the EDPS consider that the Commission should better define the purposes of general interest of such "data altruism". The EDPB and EDPS consider that this lack of definition may lead to legal uncertainty, as well as to lower the level of protection of personal data in the EU. For instance, the requirement for the data altruism organization to inform the data holder (including the data subject) "about the purposes of general interest for which it permits the processing of their data by a data user" shall be in line with the principle according to which data shall be collected for specified, explicit and legitimate purposes and not further processed in a**

[76] See recently adopted EDPB Guidelines on consent, Guidelines 5/2020, in particular on consent for scientific research, at pages 30-32.
[77] See EDPB Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak, at paras 42-45:
"42. As a general rule, data shall be "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes" pursuant to Article 5 (1) (b) GDPR.
43. However the "compatibility presumption" provided by Article 5(1)(b) GDPR states that "further processing for [...] **scientific research purposes** [...] shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes". This topic, due to its horizontal and complex nature, will be considered in more detail in the planned **EDPB guidelines on the processing of health data for the purpose of scientific research**.
44. Article 89 (1) GDPR stipulates that the processing of data for research purposes "shall be subject to **appropriate safeguards**" and that those "safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner".
45. The requirements of Article 89(1) GDPR emphasise the importance of the data minimisation principle and the principle of integrity and confidentiality as well as the principle of data protection by design and by default (see below). Consequently, considering the sensitive nature of health data and the risks when re-using health data for the purpose of scientific research, strong measures must be taken in order to ensure an appropriate level of security as required by Article 32(1) GDPR."
See also EDPB document in response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research, adopted on 2 February 2021.
[78] Recital 35: "Such purposes would include healthcare, combating climate change, improving mobility, facilitating the establishment of official statistics or improving the provision of public services. Support to scientific research, including for example technological development and demonstration, fundamental research, applied research and privately funded research, should be considered as well purposes of general interest. This Regulation aims at contributing to the emergence of pools of data made available on the basis of data altruism that have a sufficient size in order to enable data analytics and machine learning, including across borders in the Union."

manner that is incompatible with those purposes (principle of purpose limitation, under Article 5(b) of the GDPR. Hence, an exhaustive list of clearly defined purposes should be provided in the Proposal. At the same time, the EPDB and the EDPS notice the specification made in recital 38 of the Proposal[79]. These specification shall be included in the substantive part of the Proposal and not only in the recital and be accompanied by a clear distinction in the Proposal between:

- consent to areas of scientific research;

- further processing for scientific or historical or statistical purposes;

- and the processing for purposes of general interest (to be defined in the Proposal).

173. Moreover, the EDPB and the EDPS notice that the term "data repositories" in recital (36)[80], referred to only in this recital and not in the substantive part of the Proposal, and related to the processing of both personal and non-personal data, needs to be clarified.

3.5.2 Articles 16-17: registration regime - general requirements to be eligible for registration - content of the registration; outcome (and timing) of the registration;

174. Chapter IV of the Proposal establishes the possibility for organisations engaging in 'data altruism' to register as a "Data Altruism Organisation recognised in the Union"[81] with the declared aim of increasing citizens' trust in their operations. In this regard, the EDPB and EDPS underline that the Proposal does not clarify whether or not the registration is compulsory, nor whether the provisions under Chapter IV also apply in case that organisations engaging in data altruism are not registered.

175. The general requirements for registration are listed in Article 16; the requirements for registration are provided under Article 17, and notably at letters (a)-(i) of Article 17(4). The 'vetting' of the data altruism organization is limited to the verification by the competent authority of the requirements under Article 16 and 17(4) and shall occur within twelve weeks from the date of application. However, the kind of verification with which the competent authority is tasked is not defined by the Proposal.

176. In this respect, the EDPB and the EDPS remark that a regime providing stronger guarantees, in case of processing of personal data, would be more adequate to ensure appropriate checks and ultimately

[79] Recital (38): "Data Altruism Organisations recognised in the Union **should be able** to **collect relevant data directly from natural and legal persons or to process data collected by others**.
Typically, data altruism would rely on consent of data subjects in the sense of Article 6(1)(a) and 9(2)(a) and in compliance with requirements for lawful consent in accordance with Article 7 of Regulation (EU) 2016/679.
In accordance with Regulation (EU) 2016/679, **scientific research purposes** can be supported by consent to **certain areas of scientific research** when in keeping with recognised ethical standards for scientific research or only to certain areas of research or parts of research projects.
Article 5(1)(b) of Regulation (EU) 2016/679 specifies that **further processing for scientific or historical research purposes or statistical purposes** should, in accordance with Article 89(1) of Regulation (EU) 2016/679, not be considered to be incompatible with the initial purposes."
[80] Recital (36): "Legal entities that seek to support **purposes of general interest** by making available relevant data based on data altruism at scale and meet certain requirements, should be able to register as 'Data Altruism Organisations recognised in the Union'. This could lead to the establishment of **data repositories**.[...]"
[81] Recital (36) of the Proposal.

enhance trust, than the 'lighter' registration regime (almost a simply 'declaratory' regime) set out in the Proposal and similar to the one envisaged for data sharing service providers.

177. The EDPB and the EDPS underline that the fact that there is almost no requirement from a legal, technical and organizational point of view to become a "Data Altruism Organisation recognised in the Union" (or a "data sharing provider") is problematic. For instance, an organisation, entitled pursuant to Article 15(3) of the Proposal to "refer to itself as a 'Data Altruism Organisation recognised in the Union' in its written and spoken communication" ('labelling effect'), will most probably collect personal data leveraging citizens' expectations in particular on full data protection compliance by the same organisation.

178. The EDPB and the EDPS stress that data altruism organisations need to be trusted entities. As regards the general requirements for registration (provided under Article16 of the Proposal), the EDPB and EDPS also consider that the independence from the for-profit entities of the data altruism organization (e.g. legal, organizational, economical) is envisaged under Article 16(b) the Proposal should to be clarified[82].

179. **In particular, the EDPB and the EDPS recommend introducing a direct reference to data protection requirements in Article 16, especially to the technical and organizational requirements enabling the application of data protection standards and the exercise of data subjects' rights.**

180. **In light of the elements above, and considering the possible impacts for data subjects with regard to the personal data processing that may be undertaken by data altruism organisation, the EDPB and the EDPS consider that the registration regime as laid down in the Proposal does not provide for a sufficiently stringent vetting procedure applicable to such organisation. The EDPB and the EDPS recommend exploring alternative procedures which should notably take into account a more systematic inclusion of accountability and compliance tools for the processing of personal data as per the GDPR, in particular the adherence to a code of conduct or certification mechanism.**

3.5.3 Articles 18-19: transparency requirements and "specific requirements to safeguard rights and interests of data subjects and legal entities as regards their data"

181. The EDPB and the EDPS notice that the requirements accompanying the registration regime should enhance but **not replace the obligations of the data altruism organizations as controllers or processors under the GDPR**.

182. The EDPB and the EDPS notice that recital 36 of the Proposal is unclear in this regard, since it seems to imply that means to withdraw consent shall be provided by the data altruism organization acting as processor[83]. However, the qualification of data altruism organization as processor, instead of

[82] "In order to qualify for registration, the data altruism organisation shall: [...] (b) operate on a not-for-profit basis and **be independent from any entity that operates on a for-profit basis**;" (emphasis added)
[83] Recital 36 laws down (bold added): "**Further safeguards** should include making it possible to **process relevant data within a secure processing environment** operated by the registered entity, **oversight mechanisms** such as ethics councils or boards to ensure that the data controller maintains high standards of scientific ethics, **effective**

controller, needs further assessment, since it does not seem to be the only possible scenario in the context of the Proposal.

183. The enabling effect of the registration (as data altruism organisation) should also be clearly defined, especially having regard to the aspect of the legal basis for the processing of personal data under the GDPR[84]. In this regard, the EDPB and the EDPS reiterate that **the registration regime cannot replace the necessity of an appropriate legal ground for the processing of personal data under Article 6(1) of the GDPR** for the lawfulness of the data processing. In other words, according to the GDPR the processing of personal data shall be lawful only if and to the extent that at least one of the legal basis under Article 6(1) of the GDPR applies

184. Having regard to Article 18 of the Proposal, the EDPB and the EDPS have doubts as to how the independence of the data altruism organisation is preserved in cases where its funding is based on "*the fees paid by natural or legal persons processing the data*"[85] (i.e., data provided to these natural or legal persons by the data altruism organization). In addition, the EDPB and the EDPS consider that the Proposal should better explain in what situations the data altruism organisation can charge fees to natural or legal persons for the processing of the data 'conferred' by data subjects for 'data altruism'.

185. Also in this case, as remarked regarding the re-use of data held by public sector bodies, there is an issue related to incentives for the controller to encourage more processing of personal data, in this case more 'data altruism'. The qualification of data altruism organisations as registered entities having a not-for-profit character (recital 36) -which the EDPB and the EDPS welcome- only partially mitigates the aforesaid issue.

186. Moreover, the wording of recital 36 referring to requirements for data altruism organisations raises concerns since it refers to "voluntary compliance" also with regard to issues related to (mandatory) GDPR compliance[86].

---

technical means to withdraw or modify consent at any moment, **based on the information obligations of data processors under Regulation (EU) 2016/679** as well as **means for data subjects to stay informed** about the use of data they made available." (emphasis added)

[84] In this regard, recital 38 of the Proposal lays down as follows (bold added): "Data Altruism Organisations recognised in the Union **should be able to collect relevant data directly from natural and legal persons** or to process data collected by others. **Typically**, data altruism would rely on consent of data subjects in the sense of Article 6(1)(a) and 9(2)(a) and in compliance with requirements for lawful consent in accordance with Article 7 of Regulation (EU) 2016/679. In accordance with Regulation (EU) 2016/679, scientific research purposes can be supported by consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research or only to certain areas of research or parts of research projects. Article 5(1)(b) of Regulation (EU) 2016/679 specifies that further processing for scientific or historical research purposes or statistical purposes should, in accordance with Article 89(1) of Regulation (EU) 2016/679, not be considered to be incompatible with the initial purposes."

[85] See Article 18(1)(d) of the Proposal.

[86] Recital 36 (bold added): "[…] The **voluntary compliance** of such registered entities with **a set of requirements** should bring trust that the data made available on altruistic purposes is serving a general interest purpose. Such **trust** should result in particular from a **place of establishment within the Union**, as well as from the requirement that registered entities have a **not-for-profit character**, from **transparency** requirements and from **specific safeguards** in place to protect rights and interests **of data subjects and companies**. **Further safeguards** should

187. The recital is also inconsistent (unless prominence is given to the optional nature of the requirements under recital 36) with the substantive part of the Proposal, Article 17(3), which refers to data altruism organisations not established in the Union.

188. **As regards Article 19 of the Proposal, the EDPB and EDPS are of the opinion that an explicit reference to Articles 13 and 14 of the GDPR should be added, in order to ensure consistency between this Article of the Proposal and the obligations concerning the transparency principle under the GDPR, and that the necessary information is provided by the data altruism organisation and by the data users to the data subject with regard to the processing of personal data relating to her or him**.

189. Moreover, the EDPB and the EDPS consider that the current wording of Article 19(1)(a)[87] seems unclear and difficult to reconcile with the provisions of the GDPR .

190. **As regards this Chapter of the Proposal, an explicit emphasis on providing anonymized data when it is possible and adequate for the purpose of data processing, in line with the principle of data minimisation, would also be of special importance to protect persons concerned from undue risks to their fundamental rights and freedoms, especially in case of processing of special categories of data.**

3.5.4 Articles 20 and 21: competent authorities for registration and monitoring of compliance

191. **With regard to article 20(3) of the Proposal, the EDPB and the EDPS consider that the governance and monitoring of compliance should be reinforced in order to ensure a more appropriate vetting of data altruism organizations including compliance with the GDPR, and to ensure that supervision on the provisions of the Proposal is clearly defined in a way that provides that, when it is a matter of personal data, data protection requirements are fully complied with and remain under the competence of the data protection authorities established under the GDPR.**

192. **The designation of data protection authorities as the main competent authorities for the supervision and enforcement of the provisions under Chapter IV of the Proposal would also ensure a more consistent regulatory approach across Member State and therefore contribute to the consistent application of the Proposal. As per their competence and tasks under the GDPR, data protection authorities have already specific expertise in the monitoring of the compliance of data processing, the auditing of specific data processing activities and data sharing, the assessment of the adequate measures to ensure a high level of security for the storage and transmission of personal data, as well as in promoting awareness among controllers and processors of their obligation related to the processing of personal data.**

---

include making it possible to process relevant data within a **secure processing environment** operated by the registered entity, **oversight mechanisms** such as ethics councils or boards to ensure that the data controller maintains high standards of scientific ethics, effective **technical means to withdraw or modify consent** at any moment, based on the information obligations of data processors under Regulation (EU) 2016/679 as well as means for data subjects to **stay informed** about the use of data they made available."

[87] Article 19(1)(a) states (bold added): "Any entity entered in the register of recognised data altruism organisations shall inform data holders: (a) **about the purposes of general interest for which it permits the processing of their data by a data user** in an easy-to-understand manner."

193. In addition, the EDPB and EDPS consider that, when monitoring compliance, the power of the competent authorities cannot be limited to "the power to request information", as it appears from Article 21(2) of the Proposal. This limitation definitely stems from the declaratory nature of the 'labelling regime' envisaged by the Proposal, albeit it is not adequate to the level of vetting the labelling requires, due to the high expectations of data protection compliance resulting from such labelling, especially vis-à-vis data subjects.

194. The EDPB and EDPS emphasise that adequate resources should be provided to the data protection authorities in order to allow them to effectively and efficiently perform the necessary supervision. Furthermore, the EDPB and the EDPS notice in this regard that recital (28) -which refers to providers of data sharing services- states that *"this Regulation should be without prejudice to the obligation of providers of data sharing services to comply with Regulation (EU) 2016/679 and the responsibility of supervisory authorities to ensure compliance with that Regulation."* The same specification should also be made having regard to data altruism organizations.

3.5.5 Article 22: European data altruism consent form

195. Article 22 of the Proposal empowers the Commission to adopt, by means of implementing acts, a "European data altruism consent form"[88]. In this regard, Article 22, as specified under recital 41, provides that the consent form shall be established via an implementing act by the Commission, assisted by the European Data Innovation Board, in consultation with the EDPB.

196. **In this regard, the EDPB and the EDPS consider that a more binding, better structured and institutionalized mechanism than a mere consultation of the EDPB should be established by the Proposal.**

3.6 International transfers of data: Article 5(9)-(13); recital 17, 19; Article 30

197. Even if the provisions of the Proposal relating to data transfers to third countries seem *a priori* limited to only non-personal data, issues of legal and policy consistency with the EU data protection legal framework are likely to emerge during their application, in particular when personal data and non-personal data of a dataset are inextricably linked.

198. However, although the exclusion of personal data seems to be the intention of the Commission, the limitation of the scope of transfers provisions to non-personal data is not always clearly reflected by the Proposal. In particular, Article 5(9) and 5(10), related to transfers of data held by public sector bodies, could apply to personal data if those personal data are at the same time confidential data or data protected by intellectual property rights[89].

[88] Article 22(1): "In order to facilitate the collection of data based on data altruism, the Commission may adopt implementing acts developing a European data altruism consent form. The form shall allow the collection of consent across Member States in a uniform format. Those implementing acts shall be adopted in accordance with the advisory procedure referred to in Article 29 (2)."

[89] See Article 5(10) of the Proposal: "Public sector bodies shall only transmit confidential data or data protected by intellectual property rights to a re-user which intends to transfer the data to a third country other than a country designated in accordance with paragraph 9 if the re-user undertakes: (a) to comply with the obligations imposed in accordance with paragraphs 7 to 8 even after the data is transferred to the third country; and (b) to

199. **At the same time, the Proposal includes a provision (Article 5(11)) which could somehow be considered as more "protective" for non-personal data than for personal data, since according to the Proposal the Commission could ultimately adopt, by means of a delegated act[90], specific conditions for the transfer of non-personal data to certain third countries going as far as prohibition[91].**

200. **The possibility for the Commission to adopt, by means of an implementing act[92], 'adequacy decisions' for the transfer of non-personal data to a given third country is also likely to raise questions of interaction and consistency with the transfer tools provided for by the GDPR for the transfer of personal data to the same third country.**

201. **In any case, to ensure consistency with the data protection legal framework, it is important to recall in this regard that in case of 'mixed datasets' the GDPR applies, and in particular its Chapter V.**

202. The EDPB and the EDPS notice that Article 30 of the Proposal[93] refers only to non-personal data and its paragraph 2 seems to mirror the provisions of Article 48 of the GDPR (with the difference that Article 30(2) introduces a limitation in time as to the international agreements concerned).

203. According to Article 30(3) of the Proposal, entities (the public sector body, the entity to which re-use was granted, the data sharing service provider, the data altruism organisation) receiving a decision to transfer or give access to non-personal data held in the Union by a court or an administrative authority of a third country shall seek the opinion of competent authorities or bodies pursuant to the Proposal in order to determine whether the applicable transfer conditions are met (Article 30(3), last sentence).

204. The consultation of the competent authority is necessary when the decision of the court or of the administrative authority of the third country "would risk putting the addressee in conflict with Union law or with the law of the relevant Member State" (Article 30(3))[94].

205. This provision, compared with Article 48 GDPR, seems to go one step further by requiring the consultation of the competent authority in specific cases. Therefore, in this regard, it could somehow

accept the jurisdiction of the courts of the Member State of the public sector body as regards any dispute related to the compliance with the obligation in point a)."

[90] See recital (19) of the Proposal.

[91] See recital (19) of the Proposal.

[92] See Article 5(9)-(11) of the Proposal.

[93] Article 30, International access, included under Chapter VIII, final provisions.

[94] The aforesaid conditions in Article 30(3) seem sufficient to **supersede the conditions in paragraph (2), and thus supersede the international rules referred to under this paragraph**. Article 30(4) states that: "If the conditions in paragraph 2, **or 3** are met, **the public sector body, the natural or legal person to which the right to re-use data was granted under Chapter 2, the data sharing provider or the entity entered in the register of recognised data altruism organisations, as the case may be, shall, provide the minimum amount of data permissible in response to a request**, based on a reasonable interpretation of the request." (bold added). These provisions of the Proposal might be **inconsistent with other Union or member State law, notably on judicial cooperation on criminal or civil matters**. The relevance of this observation under data protection law is given by the fact that **in case of misinterpretation of the notion of non-personal data, there is a high risk of public sector bodies, data sharing service providers, data altruism organizations, data re-users and data users, transferring personal data to a third country with (significantly) lower standard of protection for the persons concerned**.

be considered as more "protective" for non-personal data than for personal data, since such notification is not envisaged under the GDPR.

3.7 Horizontal provisions on institutional settings; complaints; European Data Innovation Board (EDIB) expert group; delegated acts; penalties, evaluation and review, amendments to the single digital gateway regulation, transitional measures and entry into force

3.7.1 Article 23: requirements relating to competent authorities

206. Chapter V of the Proposal sets out the requirements for the functioning of the competent authorities designated to monitor and implement the notification framework for data-sharing service providers and entities engaged in data altruism. It stems from Chapters III and IV of the Proposal that such competent authorities are different from the data protection authorities. Indeed, the requirements established under Article 23 of the Proposal suggest a 'technical' nature of these authorities, *"legally distinct from, and functionally independent of any provider of data sharing services or entity included in the register of recognised data altruism organizations"*.

207. In this regard, the role of the data protection supervisory authorities seems limited - under Chapter III - to having a mere exchange of information with the competent authority, and - under Chapter IV- to cooperate with the latter and provide an opinion or decision regarding questions requiring an assessment of compliance with the GDPR, at the request of the competent authority. Moreover, how and to what extent data protection authorities will interact with such competent authorities is not defined by the Proposal, as well as which financial and human resources have been envisaged to allow data protection authorities to carry out the tasks required by such interaction.

208. The EDPB and the EDPS notice that many provisions of the Proposal, whose supervision is assigned to competent authorities, designated pursuant to Article 12 and 20, are related to the protection of personal data. Bearing this in mind, **the EDPB and the EDPS underline that the competences and powers of the independent supervisory authorities shall be fully respected as they are entrusted with the responsibility to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data , as established under the GDPR and EUDPR, in line with Article 16 TFEU and Article 8 of the Charter and in accordance with the relevant case law of the Court of Justice of the European Union[95]. Considering the above, the EDPB and the EDPS recommend that the Proposal explicitly acknowledge that, inasmuch as personal data is involved, data protection authorities are the main competent authorities for the monitoring of the compliance with the provisions under Chapter III and IV of the Proposal, in consultation with other relevant sectorial authorities, when necessary. As already underlined, adequate resources should be provided to these authorities to allow them to effectively and efficiently perform the necessary supervision.**

[95] See, among others, Judgment of the ECJ of 9 March 2010, *European Commission v Federal Republic of Germany*, in case C-518/07 available at: http://curia.europa.eu/juris/liste.jsf?language=en&num=C-518/07
In its judgment of 9 March 2010, the Court considered that DPAs should be free from any external influence, whether direct or indirect. The mere risk of an external influence is sufficient to conclude that the DPA cannot act with complete independence.

3.7.2 Article 24: complaints; Article 25: right to effective judicial remedy

209. The EDPB and the EDPS notice that Article 24 provides that "*Natural and legal persons shall have the right to lodge a complaint with the relevant national competent authority against a provider of data sharing services or an entity entered in the register of recognised data altruism organisations*", but does not specify the possible content of the complaint (namely, for which violation of the Proposal). It also seems that complaints against public sector bodies or re-users referred to under Chapter II of the Proposal are not possible, not foreseen under Article 24 of the Proposal.

210. In addition, Article 25 lays down the right to effective judicial remedy by any affected natural or legal person with regard to a failure to act on a complaint lodged with the competent authority, as well as with regard to decisions of competent authorities under Articles 13, 17 and 21 (respectively, decision related to supervision on data sharing services; registration of data altruism organisations; monitoring of compliance of registered data altruism organisations).

211. The EDPB and the EDPS observe that the aforesaid provisions of the Proposal on the right to lodge a complaint to the relevant national competent authority (Article 24) and on the right to an effective judicial remedy against failure to act or decisions of aforesaid competent authority (Article 25) might increase the risk, highlighted in this opinion, of parallel and inconsistent regimes between the GDPR and the Proposal. For instance, complaints related to intermediation services which provide data subjects the availability of means to exercise the rights provided under the GDPR (see Article 9(1)(b)) would fall under the remit of the competent authorities under the Proposal. In other words, the 'substantive law' inconsistencies and overlaps would also 'escalate' into administrative and judicial proceedings' overlaps of competences.

212. For this reason, **the EDPB and the EDPS call for a clear, unambiguous and rigorous definition of the substantive rules of the Proposal whose supervision is assigned to competent authorities, and of its monitoring mechanism, which ensures full consistency with the GDPR**.

3.7.3 Articles 26 and 27: composition and tasks of the European Data Innovation Board Expert Group

213. Chapter VI of the Proposal *"creates a formal expert group (the 'European Data Innovation Board') with the task of facilitating the emergence of best practices by Member States' authorities in particular on processing requests for the re-use of data which is subject to the rights of others (under Chapter II), on ensuring a consistent practice regarding the notification framework for data sharing service providers (under Chapter III), and for data altruism (Chapter IV). In addition, the formal expert group will support and advise the Commission on the governance of cross-sectoral standardisation and the preparation of strategic cross-sector standardisation requests"*[96].

[96] Explanatory Memorandum, page 8.

214. The EDPB and the EDPS notice that the newly established European Data Innovation Board, "*consisting of the representatives of competent authorities of all the Member States, the European Data Protection Board, the Commission, relevant data spaces and other representatives of competent authorities in specific sectors*" (Article 26(1)) would be entrusted with the tasks listed under Article 27, letters (a)-(e)[97], which are also relevant having regard to the processing of personal data.

215. **The EDPB and the EDPS welcome the inclusion of the EDPB as a member of the European Data Innovation Board. However, the EDPB and the EDPS consider that the provisions related to the European Data Innovation Board are likely to impinge, insofar as relating to the processing of personal data, on the tasks and competences of national data protection authorities and of the EDPB to protect the fundamental rights and freedoms of natural persons and to facilitate the free flow of personal data within the Union[98] (having regard in particular to the wide range of tasks entrusted to the EDPB under Article 70 of the GDPR to advise the Commission and to issue guidelines, recommendations and best practices, and to the tasks entrusted to the EDPS under Article 57 of the EUDPR).**

216. **Therefore, the EDPB and the EDPS recommend clarifying in the legal text that the data protection supervisory authorities established under national and Union law are the "competent authority", insofar as the processing of personal data is concerned. In addition, it should be clear that the provision of advice to the European Commission regarding data protection matters and the development of consistent practices related to the processing of personal data do not fall within the competences attributed to the European Data Innovation Board, since article 70 GDPR explicitly confers those tasks to the EDPB.**

217. **The EDPB and the EDPS also recommend, for precision and legal clarity, as well as avoidance of possible misunderstanding, renaming the European Data Innovation Board as "Commission Expert Group on Data Governance" or similar, to better reflect the *legal status* and the *nature* of the body established under Article 26 of the Proposal.**

[97] "The Board shall have the following tasks:
(a) to advise and assist the Commission in developing a consistent practice of public sector bodies and competent bodies referred to in Article 7(1) **processing requests for the re-use of the categories of data referred to in Article 3(1)**;
(b) to advise and assist the Commission in developing a consistent practice of the competent authorities in the application of **requirements applicable to data sharing providers**;
(c) to advise the Commission on the **prioritisation of cross-sector standards to be used and developed for data use and cross-sector data sharing**, cross-sectoral comparison and exchange of best practices with regards to sectoral requirements for security, access procedures, while taking into account sector-specific standardisations activities;
(d) to assist the Commission in **enhancing the interoperability of data as well as data sharing services** between different sectors and domains, building on existing European, international or national standards;
(e) to facilitate the cooperation between national competent authorities under this Regulation through capacity-building and the exchange of information, in particular by establishing methods for the efficient exchange of information relating to the notification procedure for data sharing service providers and the registration and monitoring of recognised data altruism organisations."

[98] See for instance Article 27(a), according to which the Board shall have the task to "advise and assist the Commission in developing a consistent practice of public sector bodies and competent bodies referred to in Article 7 (1) processing requests for the re-use of the categories of data referred to in Article 3 (1);" (emphasis added)

3.7.4 Article 31: penalties for infringements of the Proposal, to be applied

218. **The Proposal does not harmonize the penalties for infringements of the Proposal (nor specifies the violations that shall be sanctioned, the fines for the infringements of its provisions, nor the authorities or bodies competent to apply such penalties)**, providing that "*Member States shall lay down the rules on penalties applicable to infringements of this Regulation and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive. Member States shall notify the Commission of those rules and measures by [date of application of the Regulation] and shall notify the Commission without delay of any subsequent amendment affecting them.*"

219. The EDPB and the EDPS notice that this provision, limiting the enforceability of the Proposal (the capability to impose harmonised sanctions), and possibly also giving raise to forum-shopping for the most lenient Member State, is prejudicial to the stated aim of the Proposal to increase trust in re-use, data sharing services and data altruism.

3.7.5 Article 33: amendment to Regulation (EU) 2018/1724

220. This Article of the Proposal amends the single digital gateway regulation (Regulation (EU) 2018/1724)[99], introducing the following administrative procedures: notification as provider of data sharing services; registration as a European Data Altruism Organization. The expected outcome of which is, respectively: confirmation of the receipt of the notification, confirmation of the registration.

221. **In this regard, the EDPB and the EDPS observe that the notification and registration regime, already analysed in this Opinion, cannot replace the necessity of an appropriate legal ground for the processing of personal data under Article 6(1) of the GDPR for the lawfulness of the data processing. In other words, according to the GDPR the processing of personal data shall be lawful only if and to the extent that an adequate legal basis under Article 6(1) of the GDPR applies. The Proposal should clearly specify this aspect to avoid any ambiguity.**

Brussels, 10 March 2021

For the European Data Protection Board	For the European Data Protection Supervisor
The Chair	The European Data Protection Supervisor
(Andrea Jelinek)	(Wojciech Wiewiorowski)

[99] Regulation (EU) 2018/1724 of the European Parliament and of the Council of 2 October 2018 establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services and amending Regulation (EU) No 1024/2012 (Text with EEA relevance.), OJ L 295, 21.11.2018, p. 1–38.



SPIS TREŚCI

1 KONTEKST 4
2 OGÓLNE UZASADNIENIE DOTYCZĄCE PROJEKTU DECYZJI I PROJEKTU STANDARDOWYCH KLAUZUL UMOWNYCH 6
2.1 Ogólna struktura i metodyka wspólnej opinii 6
2.2 Ogólna prezentacja projektu decyzji oraz projektu SKU, a także ich wzajemnego oddziaływania z zaleceniami EROD dotyczącymi środków uzupełniających 7
3 ANALIZA PROJEKTU DECYZJI 8
3.1 Odniesienia do rozporządzenia (UE) 2018/1725 (motyw 8) 8
3.2 Zakres projektu decyzji i pojęcie przekazywania (art. 1 ust. 1) 9
4 ANALIZA PROJEKTU STANDARDOWYCH KLAUZUL UMOWNYCH 9
4.1 Uwaga ogólna do projektu SKU 9
4.2 Sekcja I 10
4.2.1 Klauzula 1 – Cel i zakres 10
4.2.2 Klauzula 2 – Beneficjenci będący osobami trzecimi 10
4.2.3 Klauzula 6 – Klauzula przystąpienia 12
4.3 Sekcja II – Obowiązki stron 13
4.3.1 Klauzula 1 – Zabezpieczenia w zakresie ochrony danych – moduł pierwszy (Przekazywanie między administratorami) 13
4.3.2 Klauzula 1 – Zabezpieczenia w zakresie ochrony danych – moduł drugi (Przekazywanie przez administratora podmiotowi przetwarzającemu) 15
4.3.3 Klauzula 1 – Zabezpieczenia w zakresie ochrony danych – moduł trzeci (Przekazywanie między podmiotami przetwarzającymi) 17
4.3.4 Klauzula 1 – Zabezpieczenia w zakresie ochrony danych – moduł czwarty (Przekazywanie przez podmiot przetwarzający administratorowi) 18
4.3.5 Uwagi horyzontalne – klauzula 2 (Przepisy lokalne wpływające na zapewnienie zgodności z klauzulami) oraz klauzula 3 (Obowiązki podmiotu odbierającego dane w przypadku wniosków administracji rządowej o dostęp) 19
4.3.6 Klauzula 2 – Przepisy lokalne wpływające na zapewnienie zgodności z klauzulami 20
4.3.7 Klauzula 3 – Obowiązki podmiotu odbierającego dane w przypadku wniosków administracji rządowej o dostęp 23
4.3.8 Klauzula 5 – Prawa osób, których dane dotyczą – moduł pierwszy (Przekazywanie między administratorami) 24
4.3.9 Klauzula 5 – Prawa osób, których dane dotyczą – moduły drugi (Przekazywanie przez administratora podmiotowi przetwarzającemu) i trzeci (Przekazywanie między podmiotami przetwarzającymi) 25
4.3.10 Klauzula 5 – Prawa osób, których dane dotyczą – moduł czwarty (Przekazywanie przez podmiot przetwarzający administratorowi) 26

4.3.11 Klauzula 6 – Środki zaskarżenia 26
4.3.12 Klauzula 7 – Odpowiedzialność – moduły pierwszy (Przekazywanie między administratorami) i czwarty (Przekazywanie przez podmiot przetwarzający administratorowi) 27
4.3.13 Klauzula 7 – Odpowiedzialność – moduły drugi (Przekazywanie przez administratora podmiotowi przetwarzającemu) i trzeci (Przekazywanie między podmiotami przetwarzającymi) 27
4.3.14 Klauzula 9 – Nadzór 28
4.4 Sekcja III - Postanowienia końcowe 28
4.4.1 Klauzula 1 – Brak zgodności z klauzulami i rozwiązanie umowy 28
4.5 Załączniki 28

Europejska Rada Ochrony Danych i Europejski Inspektor Ochrony Danych,

uwzględniając art. 42 ust. 2 rozporządzenia 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE,

uwzględniając Porozumienie EOG, w szczególności załącznik XI i protokół 37 do tego Porozumienia, zmienione decyzją Wspólnego Komitetu EOG nr 154/2018 z dnia 6 lipca 2018 r.[1],

PRZYJMUJĄ NINIEJSZĄ WSPÓLNĄ OPINIĘ

1 KONTEKST

1. Zgodnie z art. 44 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych[2] („**RODO**") przekazanie danych osobowych, które są przetwarzane lub mają być przetwarzane po przekazaniu do państwa trzeciego lub organizacji międzynarodowej, następuje tylko, gdy administrator i podmiot przetwarzający spełnią warunki określone w rozdziale V RODO, w tym warunki dalszego przekazania danych osobowych z państwa trzeciego lub przez organizację międzynarodową do innego państwa trzeciego lub innej organizacji międzynarodowej. W szczególności w przypadku braku decyzji stwierdzającej odpowiedni stopień ochrony każde przekazanie powinno się odbywać na podstawie odpowiednich zabezpieczeń wymienionych w art. 46 RODO.

2. Jednym z odpowiednich zabezpieczeń wymienionych w art. 46 RODO są standardowe klauzule ochrony danych przyjęte przez Komisję Europejską („**Komisja**") zgodnie z procedurą sprawdzającą, o której mowa w art. 93 ust. 2 RODO („**SKU**").

3. Aby były ważne, SKU muszą przewidywać skuteczne mechanizmy umożliwiające w praktyce zapewnienie przestrzegania wymaganego przez prawo Unii stopnia ochrony i zawieszenie lub zakazanie odbywającego się na podstawie takich klauzul przekazywania danych osobowych w przypadku ich naruszenia lub niemożności ich przestrzegania[3].

4. W dniu 15 czerwca 2001 r. Komisja przyjęła decyzję 2001/497/WE w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich, na mocy dyrektywy

[1] Odniesienia do „państw członkowskich" zawarte w niniejszej opinii należy rozumieć jako odniesienia do „państw należących do EOG".
[2] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych); Dz.U. L 119 z 4.5.2016, s. 1.
[3] Wyrok Trybunału (wielka izba) z dnia 16 lipca 2020 r.; Data Protection Commissioner/Facebook Ireland Limited i Maximillian Schrems; sprawa C-311/18; pkt 137.

95/46/WE[4], zmienioną decyzją wykonawczą Komisji (UE) 2016/2297 z dnia 16 grudnia 2016 r.[5] („**SKU z 2001 r.**"), uzupełnioną decyzją Komisji z dnia 27 grudnia 2004 r.[6] („**SKU z 2004 r.**").

5. W dniu 5 lutego 2010 r. Komisja przyjęła decyzję 2010/87/UE w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych podmiotom przetwarzającym dane mającym siedzibę w krajach trzecich na mocy dyrektywy 95/46/WE[7], zmienioną później decyzją wykonawczą Komisji (UE) 2016/2297 z dnia 16 grudnia 2016 r.[8] („**SKU z 2010 r.**").

6. W dniu 16 lipca 2020 r. Trybunał Sprawiedliwości Unii Europejskiej („**TSUE**" lub „**Trybunał**") orzekł, że badanie SKU z 2010 r. w świetle art. 7, 8 i 47 Karty praw podstawowych nie doprowadziło do żadnych ustaleń, które mogłyby mieć wpływ na ważność tej decyzji („**wyrok w sprawie Schrems II**")[9].

7. W tej samej sprawie TSUE przekazał również dodatkowe wyjaśnienia w zakresie stosowania SKU. W szczególności TSUE orzekł, że osobom, których dane dotyczą, a których dane osobowe są przekazywane do państwa trzeciego na podstawie standardowych klauzul ochrony danych, należy – podobnie jak w przypadku przekazywania na podstawie decyzji stwierdzającej odpowiedni stopień ochrony – zapewnić stopień ochrony merytorycznie równoważny temu gwarantowanemu w Unii Europejskiej[10].

8. TSUE stwierdził ponadto, że „[p]onieważ […] umowny charakter standardowych klauzul ochrony danych nierozerwalnie wiąże się z tym, że nie mogą one wiązać organów władzy publicznej państw trzecich […] może okazać się konieczne uzupełnienie tych zabezpieczeń zawartych w standardowych klauzulach ochrony danych"[11].

[4] 2001/497/WE: DECYZJA KOMISJI z dnia 15 czerwca 2001 r. w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich, na mocy dyrektywy 95/46/WE; Dz. U. L 181 z 4.7.2001, s. 19.

[5] Decyzja wykonawcza Komisji (UE) 2016/2297 z dnia 16 grudnia 2016 r. zmieniająca decyzje 2001/497/WE i 2010/87/UE w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych państwom trzecim oraz podmiotom przetwarzającym dane mającym siedzibę w takich państwach, na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady; Dz.U. L 344 z 17.12.2016, s. 100.

[6] 2004/915/WE: Decyzja Komisji z dnia 27 grudnia 2004 r. zmieniająca decyzję 2001/497/WE w zakresie wprowadzenia alternatywnego zestawu standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich; Dz.U. L 385 z 29.12.2004, s. 74.

[7] 2010/87/: Decyzja Komisji z dnia 5 lutego 2010 r. w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych podmiotom przetwarzającym dane mającym siedzibę w krajach trzecich na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady; Dz.U. L 39 z 12.2.2010, s. 5.

[8] Decyzja wykonawcza Komisji (UE) 2016/2297 z dnia 16 grudnia 2016 r. zmieniająca decyzje 2001/497/WE i 2010/87/UE w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych państwom trzecim oraz podmiotom przetwarzającym dane mającym siedzibę w takich państwach, na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady; Dz.U. L 344 z 17.12.2016, s. 100.

[9] Wyrok Trybunału (wielka izba) z dnia 16 lipca 2020 r.; Data Protection Commissioner/Facebook Ireland Limited i Maximillian Schrems; sprawa C-311/18; pkt 149.

[10] Tamże, pkt 96.

[11] Tamże, pkt 132.

9. W rezultacie w dniu 10 listopada 2020 r. EROD przyjęła Zalecenia 01/2020 dotyczące środków uzupełniających narzędzia przekazywania w celu zapewnienia zgodności z unijnym stopniem ochrony danych osobowych („**zalecenia EROD dotyczące środków uzupełniających**")[12].

10. W dniu 12 listopada 2020 r. Komisja opublikowała:

- projekt decyzji wykonawczej Komisji w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 („**projekt decyzji**") oraz
- projekt załącznika do decyzji wykonawczej Komisji w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 („**projekt SKU**").

11. W projekcie decyzji przewiduje się uchylenie SKU z lat 2001, 2004 i 2010.

12. Projekt SKU łączy klauzule ogólne z podejściem modułowym w celu uwzględnienia różnych scenariuszy przekazywania. Oprócz klauzul ogólnych administratorzy i podmioty przetwarzające powinni wybrać moduł mający zastosowanie do ich sytuacji spośród czterech poniższych wariantów:

- moduł pierwszy: przekazywanie między administratorami;
- moduł drugi: przekazywanie przez administratora podmiotowi przetwarzającemu;
- moduł trzeci: przekazywanie między podmiotami przetwarzającymi;
- moduł czwarty: przekazywanie przez podmiot przetwarzający administratorowi.

13. W tym kontekście w dniu 12 listopada 2020 r. Komisja wezwała EROD i EIOD do wydania wspólnej opinii dotyczącej projektu decyzji i projektu SKU („**wspólna opinia**") zgodnie z art. 42 ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych („**rozporządzenie (UE) 2018/1725**")[13].

2 OGÓLNE UZASADNIENIE DOTYCZĄCE PROJEKTU DECYZJI I PROJEKTU STANDARDOWYCH KLAUZUL UMOWNYCH

2.1 Ogólna struktura i metodyka wspólnej opinii

14. **Po pierwsze,** w celu zachowania przejrzystości wspólna opinia składa się z (i) części zasadniczej, w której wyszczególniono uwagi ogólne, jakie pragną przedstawić EROD i EIOD, oraz (ii) załącznika, w którym przedstawiono dodatkowe uwagi o charakterze bardziej technicznym dotyczące

[12] https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_pl.pdf

[13] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE; Dz.U. L 295 z 21.11.2018, s. 39.

bezpośrednio projektu SKU, w szczególności w celu podania kilku przykładów ewentualnych zmian. Między uwagami ogólnymi i technicznymi nie obowiązuje żadna hierarchia.

15. **Po drugie,** uwagi ogólne dotyczące projektu decyzji i projektu SKU przedstawiono w dwóch oddzielnych sekcjach. W razie potrzeby, w celu zapewnienia spójności, zamieszczono odesłania.

16. **Po trzecie,** w celu zachowania spójności w stosownych przypadkach podano również odesłania do wspólnej opinii EROD i EIOD dotyczącej standardowych klauzul umownych między administratorami a podmiotami przetwarzającymi określonych na podstawie art. 28 ust. 7 RODO i art. 29 ust. 7 rozporządzenia (UE) 2018/1725.

2.2 Ogólna prezentacja projektu decyzji oraz projektu SKU, a także ich wzajemnego oddziaływania z zaleceniami EROD dotyczącymi środków uzupełniających

17. Zasadniczo EROD i EIOD z zadowoleniem odnotowują, że projekt decyzji i projekt SKU zapewniają zwiększony poziom ochrony osób, których dane dotyczą.

18. W nawiązaniu do wkładu EROD w ocenę RODO przeprowadzoną na podstawie jego art. 97[14] EROD i EIOD z zadowoleniem przyjmują fakt, że celem tej aktualizacji istniejących SKU jest:

- dostosowanie SKU do nowych wymogów określonych w RODO[15];
- pełniejsze uwzględnienie powszechnego stosowania nowych i bardziej złożonych operacji przetwarzania, które często obejmują wiele podmiotów odbierających dane i podmiotów przekazujących dane, długie i złożone łańcuchy przetwarzania, a także zmieniające się relacje biznesowe. Oznacza to objęcie zakresem klauzul dodatkowych sytuacji przetwarzania i przekazywania danych oraz stosowanie bardziej elastycznego podejścia, np. w odniesieniu do liczby stron, które mogą przystąpić do umowy[16];
- zapewnienie specjalnych zabezpieczeń, aby uwzględnić wpływ przepisów państwa trzeciego przeznaczenia na zapewnienie zgodności z klauzulami przez podmiot odbierający dane, w szczególności w zakresie sposobu rozpatrywania wiążących wniosków organów publicznych w państwie trzecim o ujawnienie przekazywanych danych osobowych[17].

19. W szczególności EROD i EIOD z zadowoleniem przyjmują postanowienia szczegółowe, które służą uwzględnieniu najważniejszych kwestii określonych w wyroku w sprawie Schrems II, a zwłaszcza postanowienia projektu SKU dotyczące:

- przepisów prawa państwa trzeciego mających wpływ na zapewnienie zgodności z projektem SKU (sekcja II – klauzula 2);
- wniosków o udzielenie dostępu otrzymanych przez podmiot odbierający dane, złożonych przez organy publiczne państwa trzeciego (sekcja II – klauzula 3); oraz
- opcjonalnego mechanizmu dotyczącego środków zaskarżenia *ad hoc*, z którego mogą korzystać osoby, których dane dotyczą (sekcja II – klauzula 6).

[14] https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_contributiongdprevaluation_20200218.pdf
[15] Projekt decyzji wykonawczej Komisji w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679, motyw 6.
[16] Tamże, motyw 6.
[17] Tamże, motyw 18.

20. Ponadto EROD i EIOD z zadowoleniem zauważają, że w projekcie SKU odzwierciedlono szereg środków określonych w zaleceniach EROD dotyczących środków uzupełniających, choć w przypadku niektórych innych środków EROD i EIOD wzywają do zachowania większej spójności, jak opisano szczegółowo zwłaszcza w sekcji 4.3.6 poniżej.

21. W tym kontekście EROD i EIOD przypominają, że zalecenia EROD dotyczące środków uzupełniających nadal pozostaną ważne i będą miały zastosowanie po przyjęciu projektu SKU. EROD i EIOD w szczególności wzywają Komisję do wyjaśnienia, że nadal może dojść do sytuacji, w których pomimo stosowania nowych SKU będzie trzeba wprowadzać środki uzupełniające *ad hoc* w celu zapewnienia, aby osoby, których dane dotyczą, objęto ochroną na poziomie merytorycznie równoważnym temu gwarantowanemu w UE. Z tego względu nowe SKU będzie trzeba stosować równolegle z zaleceniami EROD dotyczącymi środków uzupełniających. EROD i EIOD wzywają Komisję Europejską do odniesienia się do ostatecznej wersji zaleceń EROD dotyczących środków uzupełniających, gdyby ta ostateczna wersja zaleceń została zaktualizowana przed przyjęciem projektu decyzji i projektu SKU[18].

3 ANALIZA PROJEKTU DECYZJI

3.1 Odniesienia do rozporządzenia (UE) 2018/1725 (motyw 8)

22. EROD i EIOD przyjmują do wiadomości, że motyw 8 projektu decyzji brzmi następująco:

„Ze standardowych klauzul umownych można również korzystać w przypadku przekazywania danych osobowych podwykonawcy przetwarzania w państwie trzecim przez podmiot przetwarzający niebędący instytucją unijną ani organem unijnym, przetwarzający dane osobowe w imieniu takiej instytucji unijnej lub takiego organu unijnego zgodnie z art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725. Pozwoli to również zapewnić zgodność z art. 29 ust. 4 rozporządzenia (UE) 2018/1725 w stopniu, w jakim klauzule te oraz obowiązki w zakresie ochrony danych określone w umowie lub innym akcie prawnym między administratorem a podmiotem przetwarzającym, o których to obowiązkach mowa w art. 29 ust. 3 rozporządzenia (UE) 2018/1725, są zbieżne. Będzie to dotyczyło w szczególności sytuacji, gdy administrator i podmiot przetwarzający opierają się na standardowych klauzulach umownych zawartych w decyzji […]".

23. EROD i EIOD rozumieją, że zgodnie z założeniem Komisji projekt SKU powinien objąć operacje przetwarzania między podmiotami przetwarzającymi a podwykonawcami przetwarzania, w przypadku których administratorem danych jest instytucja, organ, urząd lub agencja Unii („**instytucja Unii**") podlegające przepisom rozporządzenia (UE) 2018/1725.

24. W tym zakresie EROD i EIOD uważają, że w przypadku gdy administratorem jest instytucja Unii, w całym łańcuchu umów należy uwzględnić odpowiednie wymogi określone w rozporządzeniu (UE) 2018/1725. Kwestię tę należy doprecyzować w projekcie decyzji i projekcie SKU.

25. W każdym razie EROD i EIOD przypominają, że Komisja może zawsze usunąć wszelkie odniesienia do rozporządzenia (UE) 2018/1725, jeżeli nie zdecyduje się objąć zakresem projektu SKU określonych w art. 46 stosunków między podmiotami przetwarzającymi a podwykonawcami przetwarzania, którzy

[18] https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_pl.pdf Dokument ten przekazano do konsultacji publicznych, które trwały do dnia 21 grudnia 2020 r., i nadal podlega on możliwym dalszym zmianom wprowadzanym na podstawie tych konsultacji.

biorą udział w operacji przetwarzania, w przypadku której administratorem jest instytucja Unii objęta rozporządzeniem (UE) 2018/1725.

3.2 Zakres projektu decyzji i pojęcie przekazywania (art. 1 ust. 1)

26. **Po pierwsze,** art. 1 ust. 1 projektu decyzji stanowi, co następuje:

„Uznaje się, że standardowe klauzule umowne określone w załączniku zapewniają odpowiednie zabezpieczenia w rozumieniu art. 46 ust. 1 i art. 46 ust. 2 lit. c) rozporządzenia (UE) 2016/679 dotyczące przekazywania danych osobowych **administratorowi lub podmiotowi przetwarzającemu (podwykonawcy przetwarzania) niepodlegającemu rozporządzeniu (UE) 2016/679 (podmiot odbierający dane)** przez administratora lub podmiot przetwarzający, który podlega rozporządzeniu (UE) 2016/679 (podmiot przekazujący dane)".

27. W świetle powyższego oraz w związku z tytułem projektu decyzji EROD i EIOD rozumieją, że projekt decyzji nie obejmuje:

- przekazywania danych na potrzeby konkretnego przetworzenia, zgodnie z art. 3 ust. 2 RODO, podmiotowi odbierającemu dane spoza EOG, ale podlegającemu przepisom RODO, oraz
- przekazywania danych organizacjom międzynarodowym.

28. Mając powyższe na uwadze oraz w celu uniknięcia wątpliwości, EROD i EIOD zalecają Komisji wyjaśnienie, że postanowienia te służą jedynie uwzględnieniu kwestii zakresu projektu decyzji i projektu SKU, a nie kwestii zakresu pojęcia przekazywania danych.

29. **Po drugie,** EROD już wyjaśniła w swoich wytycznych dotyczących zakresu terytorialnego RODO[19], że administrator lub podmiot przetwarzający nigdy nie podlega jako taki przepisom RODO, a jedynie w związku z konkretną czynnością przetwarzania.

30. EROD i EIOD zalecają zatem odpowiednie przeredagowanie art. 1 ust. 1 projektu decyzji.

4 ANALIZA PROJEKTU STANDARDOWYCH KLAUZUL UMOWNYCH

4.1 Uwaga ogólna do projektu SKU

31. EROD i EIOD z zadowoleniem przyjmują wprowadzenie poszczególnych modułów dla każdego scenariusza przekazywania danych. Zauważają jednak, że nie jest jasne, czy jeden zestaw SKU może w praktyce obejmować kilka modułów dotyczących różnych sytuacji ani czy różne sytuacje wymagałyby podpisania kilku zestawów SKU. Aby osiągnąć jak największą czytelność i łatwość praktycznego zastosowania SKU, EROD i EIOD proponują, aby Komisja Europejska zapewniła dodatkowe wytyczne (np. w formie schematów działań, publikacji często zadawanych pytań (FAQ) itp.). W szczególności należy wyraźnie zaznaczyć, że połączenie różnych modułów w ramach pojedynczego zestawu SKU nie może prowadzić do rozmycia ról i obowiązków stron.

[19] https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf

4.2 Sekcja I

4.2.1 Klauzula 1 – Cel i zakres

32. Jeżeli chodzi o odniesienie do standardowych klauzul umownych, o których mowa w art. 28 ust. 7 RODO, uwzględnione w klauzuli 1 lit. c), zdaniem EROD i EIOD ważne jest, aby w projekcie decyzji jasno wyjaśnić powiązanie i zależność między przedmiotowym zbiorem SKU a SKU, o których mowa w art. 28 ust. 7 RODO. Należy wyjaśnić stronom – już w projekcie decyzji – że jeżeli zamierzają skorzystać z SKU zarówno na podstawie art. 28 ust. 7, jak i na podstawie art. 46 ust. 2 lit. c) RODO, wówczas strony muszą polegać na SKU w sprawie przekazywania danych. Zgodnie z klauzulą 1 lit. c) w projekcie SKU strony mogą wprowadzać inne klauzule lub dodatkowe zabezpieczenia, „pod warunkiem że nie są one bezpośrednio lub pośrednio sprzeczne" z projektem SKU. Aby zapewnić administratorom i podmiotom przetwarzającym pewność prawa, EROD i EIOD z zadowoleniem przyjęliby wyjaśnienia dotyczące rodzaju klauzul, które Komisja Europejska uznałaby za bezpośrednio lub pośrednio sprzeczne z projektem SKU. Wyjaśnienie takie mogłoby na przykład wskazywać, że klauzule sprzeczne z projektem SKU to takie, które podważają obowiązki określone w projekcie SKU, negatywnie na nie wpływają lub uniemożliwiają ich przestrzeganie. Na przykład klauzule zezwalające podmiotom przetwarzającym na wykorzystywanie danych do ich własnych celów byłyby sprzeczne z obowiązkiem podmiotu przetwarzającego dotyczącym przetwarzania danych osobowych wyłącznie w imieniu administratora oraz do celów i przy użyciu środków określonych przez tego ostatniego.

4.2.2 Klauzula 2 – Beneficjenci będący osobami trzecimi

33. Zgodnie z sekcją I klauzula 2 „osoby, których dane dotyczą, mogą powoływać się na te klauzule i egzekwować je jako beneficjenci będący osobami trzecimi". Prawo to dotyczy jednak wyłącznie postanowień, których nie wymieniono w tej klauzuli 2. Aby przekazać osobom, których dane dotyczą, jasne i jednoznaczne informacje na temat ich praw, a administratorom i podmiotom przetwarzającym, które będą stosowały te klauzule – na temat praw beneficjentów będących osobami trzecimi, EROD i EIOD wzywają Komisję Europejską do określenia w ramach tej klauzuli 2 wykazu pozytywnego praw możliwych do wyegzekwowania przez osoby, których dane dotyczą, zamiast wymieniania tych, których nie można wyegzekwować[20].

34. Jeżeli chodzi o treść, EROD i EIOD zauważają, że w przypadku szeregu postanowień uwzględnionych w wykazie w klauzuli 2 w praktyce to osoby, których dane dotyczą, powinny mieć możliwość ich wyegzekwowania, a zatem należałoby je wykreślić z tego wykazu.

35. EROD i EIOD uważają, że ponieważ jest tak obecnie w przypadku poprzednich zestawów SKU przyjętych przez Komisję Europejską[21] i jest to wymagane przez organy nadzorcze w odniesieniu do wiążących reguł korporacyjnych, sama **sekcja I klauzula 2 (Beneficjenci będący osobami trzecimi)** powinna podlegać egzekwowaniu przez osoby, których dane dotyczą.

36. Jeżeli chodzi o **sekcję I klauzule 3 (Wykładnia) i 4 (Hierarchia)**, należy zauważyć, że jeżeli strony nie przestrzegają zasad dotyczących wykładni i hierarchii dokumentów, może to wpłynąć na osoby,

[20] Taki wykaz byłby spójniejszy ze strukturą rozdziału III RODO, a także wcześniejszych zestawów SKU przyjętych przez Komisję Europejską (zob. klauzula 3 SKU z 2001 r.; klauzula III lit. b) SKU z 2004 r.; i klauzula 3 akapit pierwszy SKU z 2010 r.).
[21] Zob. klauzula 3 SKU z 2001 r.; klauzula III lit. b) SKU z 2004 r.; klauzula 3 SKU z 2010 r.

których dane dotyczą, i ich prawa. EROD i EIOD są zdania, że osoby, których dane dotyczą, powinny mieć możliwość wyegzekwowania tej klauzuli.

37. Takie same wymogi zawiera **sekcja II moduł drugi: klauzula 1 akapit dziewiąty lit a) oraz moduł trzeci: klauzula 1 akapit dziewiąty lit. a)**. Dotyczą one spoczywającego na podmiocie odbierającym dane obowiązku udzielania odpowiedzi na zapytania podmiotu przekazującego dane (a w przypadku modułu trzeciego również na zapytania administratora). Jeżeli dojdzie do naruszenia, EROD i EIOD uważają, że te dwie klauzule mogą mieć wpływ na osoby, których dane dotyczą, oraz ich prawa, a zatem należy uznać, że osoby takie mają możliwość ich wyegzekwowania, tak jak ma to obecnie miejsce w przypadku wcześniejszych zestawów SKU przyjętych przez Komisję Europejską[22].

38. W sekcji II moduł trzeci: klauzula 1 akapit pierwszy lit a) dotyczy obowiązku informowania podmiotu odbierającego dane przez podmiot przekazujący dane o tym, że działa on zgodnie z poleceniami administratora; w klauzuli 1 akapit pierwszy lit. b) określono obowiązek podmiotu odbierającego dane w zakresie przetwarzania danych osobowych zgodnie z poleceniami administratora oraz z poleceniami przekazanymi przez podmiot przekazujący dane; natomiast klauzula 1 akapit pierwszy lit. c) dotyczy obowiązku poinformowania podmiotu przekazującego dane przez podmiot odbierający dane, w przypadku gdy ten drugi podmiot nie jest w stanie zastosować się do tych poleceń, a także spoczywającego na podmiocie przekazującym dane obowiązku poinformowania o tym fakcie administratora. EROD i EIOD zauważają, że naruszenie postanowień **sekcji II moduł trzeci: klauzula 1 akapit pierwszy lit. a), b) i c)** może mieć wpływ na osoby, których dane dotyczą, oraz ich prawa, a zatem osoby te powinny mieć możliwość ich wyegzekwowania, tak jak ma to obecnie miejsce w przypadku wcześniejszych zestawów SKU przyjętych przez Komisję Europejską[23].

39. Jeżeli chodzi o **sekcję II moduł czwarty: klauzula 1 akapit pierwszy**, EROD i EIOD odnotowują, że klauzula 1 akapit pierwszy lit. a) i b) dotyczy spoczywającego na podmiocie przekazującym dane obowiązku odpowiednio przetwarzania danych zgodnie z poleceniami podmiotu odbierającego dane oraz informowania podmiotu odbierającego dane, jeżeli podmiot przekazujący dane nie jest w stanie działać zgodnie z poleceniami administratora lub polecenia te są sprzeczne z przepisami Unii lub państwa członkowskiego dotyczącymi ochrony danych; natomiast klauzula 1 akapit pierwszy lit. c) dotyczy spoczywającego na podmiocie odbierającym dane obowiązku powstrzymania się od podejmowania jakichkolwiek działań uniemożliwiających podmiotowi przekazującemu dane wypełnianie jego obowiązków wynikających z RODO. **Sekcja II moduł czwarty: klauzula 1 akapit trzeci** odnosi się do zdolności stron do wykazania wypełnienia zobowiązań podjętych na podstawie SKU.

40. Ponieważ naruszenie zobowiązań określonych w **sekcji II moduł czwarty: klauzula 1 akapit pierwszy lit. a), b) i c) oraz klauzula 1 akapit trzeci** mogą mieć wpływ na osoby, których dane dotyczą, oraz ich prawa, osoby te powinny mieć możliwość ich wyegzekwowania.

41. EROD i EIOD zauważają, że nieprzestrzeganie zobowiązań dotyczących podwykonawstwa przetwarzania danych może mieć wpływ na osoby, których dane dotyczą, oraz ich prawa, a zatem osoby te powinny mieć możliwość wyegzekwowania postanowień określonych w **sekcji II klauzula 4 lit. a), b) i c)**, tak jak ma to obecnie miejsce w przypadku wcześniejszych zestawów SKU przyjętych przez Komisję Europejską[24].

42. EROD i EIOD zauważają, że **sekcja II klauzula 9 lit. b)** dotyczy zgody podmiotu odbierającego dane na współpracę z właściwym organem nadzoru. Ponieważ naruszenie tego zobowiązania może mieć wpływ na osoby, których dane dotyczą, oraz ich prawa, EROD i EIOD uważają, że osoby te powinny mieć możliwość wyegzekwowania tej klauzuli, tak jak ma to obecnie miejsce w przypadku wcześniejszych zestawów SKU przyjętych przez Komisję Europejską[25], jak również wiążących reguł korporacyjnych[26].

43. EROD i EIOD zauważają, że **sekcja III klauzula 1 lit. a)** przewiduje obowiązek informowania podmiotu przekazującego dane przez podmiot odbierający dane, jeżeli nie może on zastosować się do SKU, z czego wynika obowiązek podmiotu przekazującego dane do zawieszenia przekazywania (klauzula 1 lit. b)), a następnie podmiot ten może w określonych okolicznościach rozwiązać umowę (klauzula 1 lit. c)) i poinformować podmiot odbierający dane, co stanie się z danymi po rozwiązaniu umowy (klauzula 1 lit. d)).

44. Ponieważ postanowienia te dotyczą sytuacji, w których podmiot odbierający dane nie może zastosować się do SKU lub narusza SKU, EROD i EIOD uważają, że naruszenie **sekcji III klauzula 1 lit. a), b), c) i d)** może mieć wpływ na osoby, których dane dotyczą, oraz ich prawa, a zatem osoby te powinny mieć możliwość ich wyegzekwowania, tak jak ma to obecnie miejsce w przypadku wcześniejszych zestawów SKU przyjętych przez Komisję Europejską[27], jak również wiążących reguł korporacyjnych[28].

4.2.3 Klauzula 6 – Klauzula przystąpienia

45. EROD i EIOD z zadowoleniem przyjmują włączenie do klauzuli 6 klauzuli przystąpienia, która umożliwia opcjonalnie każdemu podmiotowi przystąpienie do projektu SKU, a tym samym zostanie nową stroną umowy jako administrator lub podmiot przetwarzający. Kwalifikacja i rola stron umowy powinny być wyraźnie określone w załącznikach, zwłaszcza w przypadku przystąpienia do umowy nowych stron. W załączniku należy zatem przedstawić szczegółowy i precyzyjny podział obowiązków oraz wyraźnie wskazać, jaki rodzaj przetwarzania jest prowadzony przez który podmiot przetwarzający, w imieniu którego administratora i do jakich celów.

46. Zgodnie z klauzulą 6 lit. a) przystąpienie nowych stron do projektu SKU jest uzależnione od zgody wszystkich pozostałych stron. W celu uniknięcia trudności praktycznych EROD i EIOD z zadowoleniem

[22] Zob. klauzula 5 lit. e) SKU z 2010 r.

[23] Uwaga ta dotyczy wyłącznie sekcji II moduł trzeci: klauzula 1 akapit pierwszy lit. b) (zob. klauzula 5 lit. a) w SKU z 2010 r.) i klauzula 1 akapit pierwszy lit. c) (zob. klauzula 5 lit. b) w SKU z 2010 r.) projektu SKU. Wcześniejsze wersje SKU nie zawierają odpowiednika sekcji II moduł trzeci: klauzula 1 akapit pierwszy lit a).

[24] Zob. klauzula 5 lit. h), i) i j) SKU z 2010 r.

[25] Zob. klauzula 5 lit. c) SKU z 2001 r.; klauzula II lit. e) SKU z 2004 r.; klauzula 8 akapit drugi SKU z 2010 r.

[26] Zob. art. 47 ust. 2 lit. l) RODO. Zob. również sekcja 3.1 Dokumentu roboczego ustanawiającego tabelę zawierającą elementy i zasady, które mają zostać uwzględnione w wiążących regułach korporacyjnych (WP 256 rev.01), przyjętego przez Grupę Roboczą art. 29 i zatwierdzonego przez EROD, http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614109; oraz sekcja 3.1 Dokumentu roboczego ustanawiającego tabelę zawierającą elementy i zasady, które mają zostać uwzględnione w wiążących regułach korporacyjnych dla podmiotów przetwarzających (WP 257 rev.01), przyjętego przez Grupę Roboczą art. 29 i zatwierdzonego przez EROD, http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614110

[27] Zob. klauzula 5 lit. a) SKU z 2001 r; klauzula II lit. c) SKU z 2004 r.; klauzula 5 lit. a) i b) oraz klauzula 12 akapit pierwszy SKU z 2010 r.

[28] Zob. sekcja 6.3 Dokumentu roboczego ustanawiającego tabelę zawierającą elementy i zasady, które mają zostać uwzględnione w wiążących regułach korporacyjnych (WP 256 rev.01); oraz sekcja 6.3 Dokumentu roboczego ustanawiającego tabelę zawierającą elementy i zasady, które mają zostać uwzględnione w wiążących regułach korporacyjnych dla podmiotów przetwarzających (WP 257 rev.01).

przyjęliby objaśnienie sposobu wyrażania takiej zgody przez pozostałe strony (np. czy musi mieć formę pisemną, termin wyrażenia zgody, informacje potrzebne przed wyrażeniem zgody). EROD i EIOD z zadowoleniem przyjęliby również wyjaśnienie, czy i w jaki sposób zgodę taką muszą wyrazić wszystkie strony, niezależnie od ich kwalifikacji i roli w przetwarzaniu.

4.3 Sekcja II – Obowiązki stron

4.3.1 Klauzula 1 – Zabezpieczenia w zakresie ochrony danych – moduł pierwszy (Przekazywanie między administratorami)

4.3.1.1 Zakres modułu pierwszego (Przekazywanie między administratorami)

47. Moduł wydaje się obejmować przekazywanie między administratorami działającymi jako niezależni lub odrębni administratorzy. Aby uniknąć jakichkolwiek niejasności, EROD i EIOD wzywają Komisję do oceny i wyjaśnienia w projekcie decyzji lub w projekcie SKU, czy moduł ten dotyczy wyłącznie niezależnych lub odrębnych administratorów, czy też można go również stosować w scenariuszach dotyczących wspólnego administrowania, według których dane osobowe są przetwarzane przez współadministratorów, przy czym jeden ze tych współadministratorów ma siedzibę poza UE i nie podlega RODO.

4.3.1.2 Klauzula 1 akapit drugi – Przejrzystość

48. W klauzuli 1 akapit drugi lit. a) projektu SKU wymieniono elementy, na temat których podmiot odbierający dane musi udzielić informacji osobom, których dotyczą przekazywane dane osobowe. Aby zapewnić pełną przejrzystość i umożliwić osobom, których dane dotyczą, wykonanie przysługujących im praw przewidzianych w tej klauzuli, EROD i EIOD uważają, że wykaz elementów należy dodatkowo rozszerzyć w taki sposób, aby był zgodny z art. 14 ust. 1 i 2 RODO w odniesieniu do pośredniego gromadzenia danych. Klauzulę należy uzupełnić o informacje na temat rodzajów danych osobowych przetwarzanych przez podmiot odbierający dane oraz okresu, przez który podmiot ten będzie przechowywał dane osobowe (lub o kryteria stosowane do jego określenia).

49. Ponadto klauzula ta powinna określać termin, w którym podmiot odbierający dane ma przekazać te informacje osobom, których dane dotyczą, aby spełnić warunki określone w art. 14 ust. 3 RODO.

50. Ponadto z klauzuli 1 akapit drugi lit. b) wynika, że podmiot odbierający dane może być zwolniony z obowiązku udzielenia informacji osobom, których dane dotyczą, zgodnie z klauzulą 1 akapit drugi lit. a), w szczególności jeżeli przekazanie takich informacji okaże się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku, w którym to przypadku podmiot odbierający dane w możliwym zakresie udostępnia informacje publicznie. Wydaje się, że sformułowanie „w możliwym zakresie" nie jest zgodne z art. 14 ust. 5 lit. b) RODO i powinno zostać usunięte. W art. 14 ust. 5 lit. b) RODO nie przewidziano bowiem takiego warunku, ale określono jednoznaczny wymóg publicznego udostępnienia informacji osobie, której dane dotyczą, gdy udzielenie takich informacji okazuje się niemożliwe lub wiązałoby się z niewspółmiernie dużym wysiłkiem, bez żadnego możliwego odstępstwa.

4.3.1.3 Klauzula 1 akapit piąty – Bezpieczeństwo przetwarzania

51. W związku ze spoczywającym na podmiocie odbierającym dane obowiązkiem wdrożenia odpowiednich środków w celu zapewnienia bezpieczeństwa przekazywanych danych klauzula 1 akapit piąty lit. a) stanowi, że strony rozważają „szyfrowanie podczas przekazywania danych oraz anonimizację lub pseudonimizację, jeżeli nie uniemożliwia to osiągnięcia celu przetwarzania". W związku z odniesieniem do anonimizacji EROD i EIOD przypominają, że jeżeli dane osobowe są anonimizowane, obowiązki wynikające z RODO nie mają już zastosowania.

4.3.1.4 Klauzula 1 akapit siódmy – Dalsze przekazanie

52. Obowiązki podmiotu odbierającego dane wynikające z tej klauzuli wiążą się z kilkoma kwestiami.

53. Po pierwsze, EROD i EIOD zauważają, że klauzula ta nie zawiera zobowiązania podmiotu odbierającego dane do powiadomienia podmiotu przekazującego dane o istnieniu dalszego przekazania, tak jak określono w SKU z 2004 r. w odniesieniu do przekazywania między administratorami. EROD i EIOD nie widzą powodu, dla którego nie należałoby powtórzyć tego zobowiązania w projekcie SKU. Takie poinformowanie podmiotu przekazującego dane jest konieczne, aby podmiot ten mógł się wywiązać się z obowiązków wynikających z art. 44 RODO, które dotyczą konkretnie dalszego przekazania danych i zapewniają rozliczalność, zgodnie z wymogami RODO, za wszelkie przetwarzanie w ramach danego przetwarzania podlegającego dalszemu przekazaniu.

54. Ponadto klauzula 1 akapit siódmy stanowi, że podmiot odbierający dane może dokonać dalszego przekazania, jeżeli osoba trzecia jest związana projektem SKU lub zgadza się na takie związanie. Nie jest jednak jasne, jak to postanowienie będzie funkcjonować w praktyce, jeżeli dana osoba trzecia jest podmiotem przetwarzającym dane, w szczególności w jaki sposób będzie ona związana klauzulami, jakie wymogi będą ją obowiązywać i czy strony mogą dodać kolejny moduł (tj. moduł drugi), który dotyczyłby takiej sytuacji. Punkt ten wymaga wyjaśnienia w projekcie SKU, aby uniknąć jakichkolwiek nieporozumień w praktyce i zapewnić stronom pewność prawa. Ponadto należy sprecyzować, że osoba trzecia powinna ocenić, czy jest w stanie spełnić obowiązki określone w projekcie SKU zgodnie z przepisami państwa trzeciego mającymi zastosowanie do tej osoby trzeciej oraz, w stosownych przypadkach, wdrożyć środki uzupełniające w celu zapewnienia poziomu ochrony merytorycznie równoważnego temu wymaganemu w EOG.

55. Ponadto w klauzuli 1 akapit siódmy ppkt (iii) określono, oprócz innych warunków, że dalsze przekazanie danych może być dozwolone, jeżeli podmiot odbierający dane i osoba trzecia zawrą umowę zapewniającą „taki sam poziom ochrony danych", jak poziom określony w projekcie SKU. Według EROD i EIOD odniesienie do „takiego samego poziomu ochrony danych" nie wydaje się wystarczające, ponieważ umowa musi zasadniczo powielać te same gwarancje i obowiązki, które zawarto w projekcie SKU, aby zapewnić ciągłość ochrony zgodnie z art. 44 RODO. Klauzulę tę należy odpowiednio zmienić przez dodanie stwierdzenia, że umowa musi nakładać takie same obowiązki jak te zawarte w projekcie SKU dotyczących podmiotu przekazującego dane i podmiotu odbierającego dane. Ponadto należy w tym przypadku dodać szczególny obowiązek, zgodnie z którym strony powinny ocenić, czy są w stanie spełnić obowiązki określone w takiej umowie zgodnie z przepisami państwa trzeciego mającymi zastosowanie do tej osoby trzeciej oraz, w stosownych przypadkach, wdrożyć środki uzupełniające w celu zapewnienia poziomu ochrony merytorycznie równoważnego temu wymaganemu w EOG.

56. Ponadto należy dodać obowiązek dostarczenia przez podmiot odbierający dane osobom, których dane dotyczą, na ich wniosek, egzemplarza dokumentacji zabezpieczeń wprowadzonych na potrzeby dalszego przekazania danych. Dostarczenie egzemplarza dokumentacji takich zabezpieczeń osobom, których dane dotyczą, pomaga osiągnąć przejrzystość, która jest konieczna w związku z przekazywaniem ich danych.

57. Ponadto w klauzuli 1 akapit siódmy ppkt (iv) określono, że dalsze przekazanie danych może nastąpić, jeżeli podmiot odbierający dane uzyskał wyraźną zgodę osoby, której dane dotyczą. Możliwość działania na podstawie zgody osoby, której dane dotyczą, odpowiada odstępstwu dotyczącemu szczególnych sytuacji określonych w art. 49 ust. 1 lit. a) RODO. EROD i EIOD są zdania, że w projekcie SKU należy wskazać, że taka możliwość ma charakter odstępstwa i wyjątku, w szczególności w porównaniu z innymi możliwymi podstawami dalszego przekazania danych, o których mowa w tej klauzuli. W związku z tym należy sprecyzować, że zgoda osoby, której dane dotyczą, mogłaby – w drodze wyjątku – stanowić podstawę dalszego przekazania danych tylko wtedy, gdy nie można skorzystać z innych mechanizmów wymienionych w klauzuli 1 akapit siódmy. Ponadto EROD i EIOD są

zdania, że Komisja powinna ocenić możliwość dalszego przekazania danych, w szczególności jeżeli jest ono niezbędne do ustalenia, dochodzenia lub obrony roszczeń oraz do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej.

4.3.2 Klauzula 1 – Zabezpieczenia w zakresie ochrony danych – moduł drugi (Przekazywanie przez administratora podmiotowi przetwarzającemu)

4.3.2.1 Klauzula 1 akapit piąty – Ograniczenie przechowywania oraz usunięcie lub zwrot danych

58. Klauzula 1 akapit piąty projektu SKU stanowi, że po zakończeniu świadczenia usług przetwarzania danych podmiot odbierający dane usuwa wszystkie dane osobowe przetwarzane w imieniu podmiotu przekazującego dane (wariant 1) lub zwraca podmiotowi przekazującemu dane wszystkie dane osobowe przetwarzane w jego imieniu i usuwa istniejące kopie (wariant 2). EROD i EIOD są zdania, że takie sformułowanie jest sprzeczne z art. 28 ust. 3 lit. g) RODO, który stanowi, że usunięcie lub zwrot danych odbywają się „zależnie od decyzji administratora". W związku z tym klauzula 1 akapit piąty powinna stanowić, że usunięcie lub zwrot danych osobowych następuje zależnie od decyzji podmiotu przekazującego dane działającego jako administrator, aby rozwiać wszelkie wątpliwości, że decyzja ta nie należy do podmiotu odbierającego dane działającego jako podmiot przetwarzający.

59. Ponadto klauzula ta stanowi, że jeżeli podmiot odbierający dane nie usunie lub nie zwróci danych podmiotowi przekazującemu dane ze względu na lokalne wymogi mające zastosowanie do podmiotu odbierającego dane, podmiot odbierający dane zagwarantuje poziom ochrony wymagany w projekcie SKU „w możliwym zakresie". EROD i EIOD uważają, że jeżeli dane mają być przechowywane przez podmiot odbierający dane, ochronę przewidzianą w projekcie SKU należy zapewnić w pełni i bez wyjątków, aby zagwarantować ciągłość ochrony. W związku z tym z klauzuli tej należy usunąć sformułowanie „w możliwym zakresie".

60. Ponadto klauzula 1 akapit piąty stanowi, że spoczywający na podmiocie odbierającym dane obowiązek zwrotu lub usunięcia danych osobowych ma zastosowanie bez względu na wszelkie wymogi „wynikające z prawa lokalnego", które zabrania zwrotu lub zniszczenia danych. Takie sformułowanie jest sprzeczne z art. 28 ust. 3 lit. g) RODO. Komisja powinna zawrzeć w projekcie SKU wyjaśnienie, że w klauzuli tej należy uwzględnić wyłącznie wymogi przewidziane w przepisach lokalnych nienaruszające istoty podstawowych praw i wolności oraz niewykraczające poza to, co jest konieczne i proporcjonalne w społeczeństwie demokratycznym do osiągnięcia jednego z celów wymienionych w art. 23 ust. 1 RODO. EROD i EIOD uważają, że w załączniku I pkt B należy wyraźnie określić szczegółowe wymogi prawne dotyczące okresów zatrzymywania danych ustanowionych w przepisach lokalnych, rodzajów danych i okresów zatrzymywania.

4.3.2.2 Klauzula 1 akapit szósty – Bezpieczeństwo przetwarzania danych

61. Podobnie jak w module pierwszym, w klauzuli 1 akapit szósty lit. a) określono, że w celu zapewnienia bezpieczeństwa przekazywanych danych strony rozważają „szyfrowanie podczas przekazywania danych oraz anonimizację lub pseudonimizację, jeżeli nie uniemożliwia to osiągnięcia celu przetwarzania". W związku z odniesieniem do anonimizacji EROD i EIOD przypominają, że jeżeli dane osobowe są anonimizowane, obowiązki wynikające z RODO nie mają już zastosowania.

62. Ponadto klauzula 1 akapit szósty lit. d) przewiduje, że podmiot odbierający dane ma obowiązek współpracować „w dobrej wierze" i wspierać podmiot przekazujący dane w wypełnianiu jego obowiązków wynikających z RODO. Pojęcia „w dobrej wierze" nie stosuje się w innych częściach SKU, w których wspomina się o obowiązku współpracy, a EROD i EIOD nie widzą potrzeby takiego doprecyzowania, które w każdym razie wykraczałoby poza przepisy RODO w tej kwestii. Należy je zatem skreślić.

4.3.2.3 Klauzula 1 akapit ósmy – Dalsze przekazywanie

63. Do klauzuli 1 akapit ósmy ppkt (i) należy dodać obowiązek dostarczenia przez podmiot odbierający dane podmiotowi przekazującemu dane, na jego wniosek, egzemplarza dokumentacji zabezpieczeń wprowadzonych w celu uzasadnienia dalszego przekazania danych osobie trzeciej. Obowiązek taki przewidziano w SKU z 2010 r. między administratorem a podmiotem przetwarzającym. EROD i EIOD nie widzą powodu wyłączenia go z proponowanego projektu SKU, ponieważ przedstawienie tych zabezpieczeń stanowi istotny element spoczywającego – na mocy RODO – na podmiocie przekazującym dane obowiązku zapewnienia rozliczalności w odniesieniu do przekazania, którego ten podmiot dokonuje, w tym dalszego przekazania.

64. Należy dodać również obowiązek dostarczenia przez podmiot odbierający dane osobom, których dane dotyczą, na ich wniosek, egzemplarza dokumentacji tych zabezpieczeń, tak jak ma to miejsce w przypadku SKU z 2010 r. między administratorem a podmiotem przetwarzającym. Tak jak powyżej, EROD i EIOD nie widzą powodu, dla którego należałoby wyłączyć to zobowiązanie z proponowanego projektu SKU. Dostarczenie dokumentacji takich zabezpieczeń osobom, których dane dotyczą, pomaga osiągnąć przejrzystość, która jest konieczna w związku z przekazywaniem ich danych.

4.3.2.4 Klauzula 1 akapit dziewiąty – Dokumentacja i przestrzeganie zobowiązań

65. W **klauzuli 1 akapit dziewiąty lit. d)** w projekcie SKU przewidziano możliwość skorzystania przez podmiot przekazujący dane, w celu przeprowadzania audytów, z usług niezależnego audytora wyznaczonego przez podmiot odbierający dane. Przepis ten nie jest przewidziany w art. 28 ust. 3 lit. h) RODO i należy go dostosować do tego artykułu, który stanowi, że podmiot przetwarzający musi umożliwić administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczynić się do nich[29]. W związku z tym podmiot przetwarzający może zaproponować audytora, ale decyzję o jego wyborze należy pozostawić administratorowi zgodnie z art. 28 ust. 3 lit. h) RODO. Administrator powinien od samego początku mieć swobodę wyboru audytora. Klauzula 1 akapit dziewiąty lit. d) stanowi również, że jeżeli podmiot przekazujący dane zleca przeprowadzenie audytu niezależnemu audytorowi, ponosi koszty jego wynagrodzenia, a jeżeli podmiot odbierający dane zleca przeprowadzenie audytu – musi on ponieść koszty wynagrodzenia niezależnego audytora. Ponieważ kwestia podziału kosztów między administratora a podmiot przetwarzający nie jest uregulowana w RODO, EROD i EIOD uważają w związku z tym, że z klauzuli tej należy usunąć wszelkie odniesienia do kosztów. Ta sama uwaga dotyczy odpowiedniego postanowienia w module trzecim.

[29] Ponieważ EROD wymaga tego obecnie w kontekście wiążących reguł korporacyjnych dotyczących podmiotów przetwarzających, zob. dokument WP 257 (zatwierdzony przez EROD), sekcja 2.3 „Każdy podmiot przetwarzający lub podprzetwarzający dane osobowe w imieniu konkretnego administratora wyrazi zgodę, na wniosek tego administratora, na przeprowadzenie audytu w swoich obiektach przetwarzania danych w odniesieniu do prowadzonych przez tego administratora czynności przetwarzania, przy czym taki audyt przeprowadzany jest przez administratora lub organ kontrolny złożony z niezależnych członków posiadających wymagane kwalifikacje zawodowe, związanych obowiązkiem zachowania poufności, wybranych przez administratora danych, w stosownych przypadkach w porozumieniu z organem nadzorczym.": https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49726
https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49726

4.3.3 Klauzula 1 – Zabezpieczenia w zakresie ochrony danych – moduł trzeci (Przekazywanie między podmiotami przetwarzającymi)

66. Zgodnie z klauzulą 1 akapit pierwszy podmiot odbierający dane jest zobowiązany do przetwarzania danych osobowych wyłącznie zgodnie z poleceniami administratora. Ponadto art. 28 ust. 4 RODO wymaga, że jeżeli do wykonania w imieniu administratora konkretnych czynności przetwarzania podmiot przetwarzający korzysta z usług innego podmiotu przetwarzającego/podwykonawcy przetwarzania, na ten inny podmiot przetwarzający nałożone zostają – na mocy umowy lub innego aktu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego – „te same obowiązki ochrony danych jak w umowie lub innym akcie prawnym między administratorem a podmiotem przetwarzającym", o których to obowiązkach mowa w art. 28 ust. 3 RODO. EROD i EIOD są zdania, że strony muszą uwzględnić wymóg zawarty w art. 28 ust. 4 RODO również w tym scenariuszu.

4.3.3.1 Klauzula 1 akapit pierwszy – Polecenia

67. Moduł trzeci dotyczy przekazywania między przetwarzającymi. W związku z tym osoby zajmujące się tą kwestią mogą początkowo zakładać, że umowa na mocy art. 46 RODO może zostać zawarta wyłącznie między przetwarzającym a jego podmiotem przetwarzającym/podwykonawcą przetwarzania, jeżeli opiera się wyłącznie na module trzecim. W klauzuli 1 akapit pierwszy lit. a) odniesiono się jednak do załącznika I pkt A i wykazu „stron", który obejmuje tożsamość i dane kontaktowe administratora oraz jego podpis. EROD i EIOD są zdania, że Komisja musi wyjaśnić, czy administrator musi podpisać te klauzule, czy też podmiot przetwarzający i podwykonawca przetwarzania muszą jedynie podać tożsamość administratora w załączniku. W pierwszym przypadku należy wyjaśnić, jaki miałoby to wpływ na administratora i które obowiązki określone w module trzecim miałyby do niego zastosowanie.

68. Ponadto klauzula 1 akapit pierwszy stanowi, że podmiot przekazujący dane może udzielać dalszych poleceń dotyczących przetwarzania danych „w ramach umowy uzgodnionej z podmiotem odbierającym dane przez cały okres obowiązywania umowy". Nie jest jasne, czy odniesienie do ram umowy w jakikolwiek sposób ogranicza prawo administratora do wydawania dalszych poleceń dotyczących przetwarzania danych, tym bardziej, że klauzula 7 projektu SKU opartych na art. 28 nie zawiera takiego możliwego ograniczenia. Klauzula 7 stanowi po prostu, że „administrator może również wydawać dalsze polecenia przez cały okres przetwarzania danych osobowych".

4.3.3.2 Klauzula 1 akapit piąty – Ograniczenie przechowywania oraz usunięcie lub zwrot danych

69. Klauzula 1 akapit piąty stanowi, że po zakończeniu świadczenia usług przetwarzania danych podmiot odbierający dane usuwa wszystkie dane osobowe przetwarzane w imieniu podmiotu przekazującego dane (wariant 1) lub zwraca podmiotowi przekazującemu dane wszystkie dane osobowe przetwarzane w jego imieniu i usuwa istniejące kopie (wariant 2). EROD i EIOD są zdania, że takie sformułowanie jest sprzeczne z art. 28 ust. 3 lit. g) RODO, który stanowi, że usunięcie lub zwrot danych odbywają się „zależnie od decyzji administratora". W związku z tym klauzula 1 akapit piąty powinna stanowić, że usunięcie lub zwrot danych osobowych następuje zależnie od decyzji administratora. Ponadto w wariancie 2 należy dodać, że podmiot odbierający dane powinien być zobowiązany do poświadczenia podmiotowi przekazującemu dane, że usunął istniejące kopie danych.

70. Ponadto klauzula 1 akapit piąty stanowi, że spoczywający na podmiocie odbierającym dane obowiązek zwrotu lub usunięcia danych osobowych ma zastosowanie bez względu na wszelkie wymogi „wynikające z prawa lokalnego", które zabrania zwrotu lub zniszczenia danych. Takie sformułowanie jest sprzeczne z art. 28 ust. 3 lit. g) RODO. Biorąc pod uwagę, że podmiot przetwarzający podlega przepisom państwa trzeciego, a zatem może być prawnie zobowiązany do (dalszego) przechowywania danych (np. do celów księgowych), EROD i EIOD uważają, że Komisja powinna zawrzeć w projekcie SKU wyjaśnienie, że w klauzuli tej należy uwzględnić wyłącznie wymogi przewidziane w przepisach lokalnych nienaruszające istoty podstawowych praw i wolności oraz niewykraczające poza to, co jest konieczne i proporcjonalne w społeczeństwie demokratycznym do osiągnięcia jednego z celów wymienionych w art. 23 ust. 1 RODO. Tak jak w module drugim, EROD i EIOD uważają, że w załączniku I pkt B należy wyraźnie określić szczegółowe wymogi prawne dotyczące okresów zatrzymywania danych ustanowionych w przepisach lokalnych, rodzajów danych i okresów zatrzymywania.

Ponadto należy usunąć sformułowanie „w możliwym zakresie". Aby uniknąć powtórzeń, EROD i EIOD zachęcają Komisję do wprowadzenia odniesienia do sekcji 4.3.2.1.

4.3.3.3 Klauzula 1 akapit piąty – Bezpieczeństwo przetwarzania oraz klauzula 1 akapit szósty – Szczególne kategorie danych osobowych

71. Aby uniknąć powtórzeń, EROD i EIOD zachęcają Komisję do wprowadzenia odniesienia do uwag przedstawionych w sekcji 4.3.2.2.

4.3.4 Klauzula 1 – Zabezpieczenia w zakresie ochrony danych – moduł czwarty (Przekazywanie przez podmiot przetwarzający administratorowi)

72. EROD i EIOD przyjmują do wiadomości, że zakres modułu czwartego obejmuje wyłącznie przekazywanie danych przez podmiot przetwarzający podlegający RODO jego własnemu administratorowi niepodlegającemu RODO, a wyklucza przekazywanie danych przez taki podmiot przetwarzający jakiemukolwiek innemu administratorowi, jak wyjaśniono w art. 1 ust. 1 i motywie 16 projektu decyzji. Niemniej, aby uniknąć wszelkich nieporozumień co do zakresu tego modułu, EROD i EIOD zalecają umieszczenie krótkiego wyjaśnienia dotyczącego ograniczenia zakresu modułu czwartego w samym projekcie SKU.

73. EROD i EIOD z zadowoleniem przyjęliby wszelkie dodatkowe wyjaśnienia na temat modułu czwartego, jakie Komisja Europejska mogłaby zawrzeć w projekcie decyzji, tak aby lepiej zrozumieć przesłanki, na których oparto się przy ustalaniu, które zobowiązania powinny zostać podjęte przez strony korzystające z modułu czwartego.

74. Aby zapewnić zgodność ze wszystkimi niezbędnymi przepisami art. 28 RODO mającymi bezpośrednie zastosowanie do podmiotu przetwarzającego, moduł czwarty należy uzupełnić w sposób określony poniżej.

75. Należy uwzględnić zobowiązanie podmiotu przetwarzającego do zapewnienia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy (art. 28 ust. 3 lit. b) RODO).

76. Do przedmiotowego modułu SKU należy również dodać klauzulę dotyczącą nałożenia na podmiot przetwarzający na podstawie art. 33 ust. 2 RODO obowiązku zgłaszania naruszenia ochrony danych osobowych.

77. Ponadto do modułu należy dodać klauzulę dotyczącą zlecania podwykonawstwa przetwarzania przez podmiot przetwarzający/przekazujący dane, ponieważ jest to bezpośredni obowiązek podmiotu przetwarzającego dane wynikający z art. 28 ust. 3 i 4 RODO.

78. Strony muszą również zobowiązać się do wzajemnej pomocy i wsparcia. Oprócz zobowiązania określonego już w klauzuli 5 w module czwartym, dotyczy to również obowiązku podmiotu przetwarzającego dane dotyczącego informowania administratora o naruszeniach ochrony danych osobowych (art. 33 ust. 2 RODO), który należy wyraźnie zawrzeć w umowie.

4.3.5 Uwagi horyzontalne – klauzula 2 (Przepisy lokalne wpływające na zapewnienie zgodności z klauzulami) oraz klauzula 3 (Obowiązki podmiotu odbierającego dane w przypadku wniosków administracji rządowej o dostęp)

4.3.5.1 Częściowe zwolnienie ze stosowania modułu czwartego

79. Ponieważ klauzule 2 i 3 będą miały zastosowanie do modułu czwartego „tylko jeżeli unijny podmiot przetwarzający połączy dane osobowe otrzymane od administratora z państwa trzeciego z danymi osobowymi zebranymi przez podmiot przetwarzający w UE". EROD i EIOD podkreślają, że art. 3 ust. 1 RODO nie stanowi, że dane osobowe przetwarzane przez podmiot przetwarzający w UE muszą być (również) zebrane w UE, aby miały do nich zastosowanie obowiązki dotyczące podmiotu przetwarzającego. EROD i EIOD wzywają zatem Komisję do wyjaśnienia powodów, dla których wprowadzono to zwolnienie, oraz do dalszego zbadania, czy jest ono uzasadnione.

80. Ponadto EROD i EIOD wzywają Komisję do wyjaśnienia pojęcia „połączenia" danych osobowych otrzymanych od administratora z państwa trzeciego z danymi osobowymi zebranymi przez podmiot przetwarzający w UE oraz sytuacji, w których takie połączenie będzie miało miejsce, ponieważ w RODO nie przewidziano takiego pojęcia połączenia danych.

4.3.5.2 Sytuacje objęte klauzulami 2 i 3

81. W odniesieniu do sytuacji, o których mowa w klauzulach 2 i 3, EROD i EIOD zauważają, że należy wyjaśnić zakres stosowania tych postanowień. Nie jest do końca jasne, czy klauzule te obejmują sytuacje, w których w przypadku braku przepisów państwa trzeciego wpływających na zgodność z zobowiązaniami podmiotu odbierającego dane praktyki wpływające na taką zgodność nadal musiałyby być brane pod uwagę i oceniane, ani nawet czy klauzule te obejmą praktyki odbiegające od tego, co przewidują ramy prawne państwa trzeciego. Na przykład nawet jeżeli dostęp organów publicznych państwa trzeciego do danych nie jest przewidziany w mających zastosowanie ramach prawnych, dostęp taki może mieć miejsce w praktyce lub organy mogą uzyskać dostęp do danych z pominięciem ram prawnych. Aby wyraźnie uwzględnić te sytuacje, należy odpowiednio zmienić tytuły tych klauzul (w szczególności należy uzupełnić tytuł klauzuli 2, która odnosi się wyłącznie do przepisów) oraz doprecyzować brzmienie klauzul.

82. W szczególności wydaje się, że w klauzuli 2 lit. a) nie nakłada się żadnych szczególnych obowiązków, w przypadku gdy nie obowiązują żadne przepisy dotyczące dostępu organów publicznych do danych osobowych. W tym względzie należy przypomnieć, że w zaleceniach EROD dotyczących środków uzupełniających wskazano, że w przypadku braku publicznie dostępnych przepisów podmiot przekazujący dane powinien mimo wszystko zbadać inne istotne i obiektywne czynniki. Uzasadnieniem tego zalecenia jest fakt, że w przypadku braku przepisów dotyczących dostępu organów publicznych do danych osobowych nie można racjonalnie zakładać, że w praktyce taki dostęp nie ma miejsca.

83. Z tego względu EROD i EIOD zalecają uzupełnienie klauzul 2 i 3 w taki sposób, aby istniały również zabezpieczenia dotyczące sytuacji, gdy w państwie trzecim nie obowiązują przepisy w tym zakresie, ale gdy takie praktyki – które byłyby wówczas sprzeczne z wymogami UE w zakresie ochrony danych – mają miejsce lub gdy praktyka będzie odbiegać od przepisów ram prawnych. W szczególności należy zatem wyjaśnić w projekcie SKU, że w przypadku braku przepisów w państwie trzecim dotyczących dostępu organów publicznych do danych osobowych strony powinny mimo to, opierając się na wszelkich dostępnych informacjach, dążyć do zidentyfikowania wszelkich praktyk mających zastosowanie do przekazywanych danych, które uniemożliwiają podmiotowi odbierającemu dane wypełnianie jego obowiązków.

4.3.5.3 Zakres klauzul 2 i 3

84. Również w kwestii zakresu klauzul EROD i EIOD zauważają, że niektóre elementy są niejednoznaczne, np.: odniesienie w klauzuli 2 lit. b) do „braku wniosków o ujawnienie danych otrzymanych przez podmiot odbierający dane od organów publicznych" lub do „odpowiedniego doświadczenia praktycznego" w tym zakresie, jak również użycie czasu teraźniejszego w klauzuli 2 lit. e) w odniesieniu do momentu, w którym odbierający dane „podlega lub zaczął podlegać przepisom prawa niezgodnym z wymogami określonymi w lit. a)" klauzuli 2. Elementy te mogą stwarzać wrażenie, że przekazywanie nadal może mieć miejsce, chociaż z wcześniejszej oceny ram prawnych państwa trzeciego podmiotu odbierającego dane wynika, że przepisy państwa trzeciego nie są zgodne z wymogami UE dotyczącymi poziomu ochrony danych osobowych i że nie można wprowadzić skutecznych środków uzupełniających. EROD i EIOD zalecają zatem doprecyzowanie, że klauzule te będą miały zastosowanie wyłącznie do sytuacji, w których w momencie zawierania umowy oceniono, że odpowiednie prawo lub prawa państwa trzeciego zapewniają poziom ochrony merytorycznie równoważny temu gwarantowanemu w UE, albo gdy wprowadzono skuteczne środki uzupełniające w celu zaradzenia potencjalnym brakom stwierdzonym w tych przepisach lub praktykach oraz w celu zapewnienia skutecznego stosowania zabezpieczeń zawartych w projekcie SKU, tak aby umożliwić podmiotowi odbierającemu dane wywiązanie się z jego obowiązków, lub gdy państwo trzecie nie posiada żadnego prawa w dziedzinie związanej z przekazywanymi danymi.

85. Innymi słowy, mechanizmy przewidziane w tych klauzulach będą uruchamiane wyłącznie w przypadkach, gdy:

- państwo trzecie nie posiada odpowiednich przepisów, ale zostanie ujawniona praktyka niezgodna z wymogami UE;
- w państwie trzecim dojdzie do zmiany przepisów, w rezultacie czego ramy prawne państwa trzeciego podmiotu odbierającego dane nie będą już zapewniały merytorycznie równoważnego poziomu ochrony danych, co będzie wymagało zawieszenia przekazywania prowadzonego na podstawie SKU; albo
- w praktyce prawo będzie stosowane inaczej i nie będzie już zapewniać poziomu ochrony merytorycznie równoważnego temu gwarantowanemu w UE.

4.3.6 Klauzula 2 – Przepisy lokalne wpływające na zapewnienie zgodności z klauzulami

4.3.6.1 Obiektywna ocena przepisów państwa trzeciego

86. EROD i EIOD podkreślają, że ocena, czy w prawie lub praktyce państwa trzeciego przeznaczenia istnieje jakikolwiek element, który uniemożliwia podmiotowi odbierającemu dane wypełnianie obowiązków wynikających z projektu SKU w kontekście określonego przekazywania, powinna opierać się na czynnikach obiektywnych, niezależnie od prawdopodobieństwa dostępu do danych osobowych. Jak podkreślono w zaleceniach EROD dotyczących środków uzupełniających (w szczególności w pkt 33 i 42)[30], ocena ta zależy od okoliczności przekazywania, a w szczególności od następujących czynników obiektywnych:

[30] https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_pl.pdf

- celów, w jakich dane są przekazywane i przetwarzane (np. marketing, HR, przechowywanie, wsparcie informatyczne, badania kliniczne);
- rodzajów podmiotów zaangażowanych w przetwarzanie (prywatne czy publiczne; administrator czy podmiot przetwarzający);
- sektora, w którym przekazywanie ma miejsce (np. adtech, telekomunikacja, sektor finansowy itd.);
- kategorii przekazywanych danych osobowych (np. dane osobowe dotyczące dzieci mogą być objęte zakresem stosowania przepisów szczególnych w państwie trzecim);
- tego, czy dane będą przechowywane w państwie trzecim i czy do danych przechowywanych w UE/EOG możliwy będzie tylko dostęp zdalny;
- formatu danych, które będą przekazywane (tj. czy dane będą w formie zwykłego tekstu, spseudonimizowane lub zaszyfrowane);
- możliwości dalszego przekazywania danych z jednego państwa trzeciego do innego państwa trzeciego.

87. W tym względzie EROD i EIOD przypominają również, że w wyroku w sprawie Schrems II TSUE nie odniósł się do żadnego czynnika subiektywnego, takiego jak na przykład prawdopodobieństwo dostępu. Sam fakt, że dane wchodzą w zakres stosowania przepisów państwa trzeciego, które dopuszczają dostęp organów publicznych do danych bez szczególnych niezbędnych gwarancji (jak przypomniano w zaleceniach EROD 02/2020 dotyczących niezbędnych gwarancji europejskich dla środków nadzoru[31]), oznacza w efekcie uznanie, że taki dostęp prawdopodobnie będzie miał miejsce, bez potrzeby opierania się na jakichkolwiek praktycznych doświadczeniach w tym zakresie lub braku otrzymania przez podmiot odbierający dane wniosków o ujawnienie danych ze strony organów publicznych. Obecne brzmienie klauzuli 2 lit. b) ppkt (i) może być zatem źle zrozumiane, ponieważ można ją odczytać jako dopuszczenie przekazania danych, jeżeli podmiot odbierający dane nie otrzymał jeszcze żadnego nakazu ujawnienia danych osobowych, nawet jeżeli podlega on lokalnym przepisom, które umożliwiają takie nakazy. Mogłoby to być również rozumiane jako przyzwolenie na kontynuowanie przekazywania danych, w przypadku gdy podmiot odbierający dane po prostu nie może udzielić podmiotowi przekazującemu dane informacji na ten temat ze względu na zakaz wypowiedzi. Ponadto ocena tego rodzaju czynników subiektywnych (prawdopodobieństwo dostępu) w praktyce byłaby bardzo skomplikowana i trudna do zweryfikowania.

88. W związku z tym EROD i EIOD zalecają:

- skreślenie odniesienia do „treści i okresu obowiązywania umowy"; „skali i regularności przekazywania"; „liczby zaangażowanych podmiotów i wykorzystywanych kanałów transmisji"; „wszelkich istotnych doświadczeń praktycznych dotyczących wcześniejszych przypadków lub braku otrzymania przez podmiot odbierający dane wniosków o ujawnienie danych ze strony organów publicznych";
- zapewnienie pełnej spójności między klauzulą 2 lit. b) ppkt (i) a zaleceniami EROD dotyczącymi środków uzupełniających;
- odpowiednią zmianę klauzuli 2 lit. b) ppkt (ii).

[31] https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_pl.pdf

4.3.6.2 Nowy załącznik do projektu SKU

89. W celu uniknięcia sytuacji, w której strony jedynie zgadzają się na udokumentowanie wspomnianej powyżej oceny, ale nie robią tego w praktyce, EROD i EIOD zalecają dodanie załącznika do projektu SKU, aby nałożyć na strony obowiązek udokumentowania, przed podpisaniem umowy, oceny przeprowadzonej zgodnie z klauzulą 2 (tj. oceny przepisów i praktyk państwa trzeciego w świetle okoliczności przekazywania). Pomogłoby to w zapewnieniu prawidłowego stosowania projektu SKU, ponieważ jednoznaczny załącznik zwróciłby uwagę podmiotów przekazujących dane i podmiotów odbierających dane na konieczność przeprowadzenia takiej oceny.

4.3.6.3 Konsultacje z organem nadzorczym w sprawie środków uzupełniających

90. Zgodnie z klauzulą 2 lit. f) projekt SKU przewiduje konsultacje z właściwym **organem nadzorczym**. Jak podkreślono w zaleceniach EROD dotyczących środków uzupełniających, „[j]eśli zamierzają Państwo wprowadzić środki uzupełniające w dodatku do standardowych klauzul umownych, nie ma potrzeby składania wniosku do właściwego organu nadzorczego o pozwolenie na dodanie tego rodzaju klauzul lub dodatkowych zabezpieczeń, o ile określone środki uzupełniające nie są w bezpośredniej lub pośredniej sprzeczności ze standardowymi klauzulami umownymi i są wystarczające, żeby zapewnić, iż stopień ochrony gwarantowany przez RODO nie zostanie naruszony"[32].

91. W istocie to podmiot przekazujący dane, z pomocą podmiotu odbierającego dane, jest odpowiedzialny za określenie tych środków. Jest to zgodne z zasadą rozliczalności zawartą w art. 5 ust. 2 RODO, który wymaga, aby administratorzy byli odpowiedzialni za przestrzeganie zasad dotyczących przetwarzania danych osobowych określonych w RODO i byli w stanie wykazać, że ich przestrzegają. Podkreślił to TSUE w wyroku w sprawie Schrems II[33] i przywołano to w zaleceniach EROD dotyczących środków uzupełniających[34].

92. Ponadto EROD i EIOD podkreślają, że w RODO nie ma wyraźnej podstawy prawnej, zgodnie z którą organy nadzorcze musiałyby zapewnić tego rodzaju konsultacje.

4.3.6.4 Powiadamianie organów nadzorczych w sytuacji, gdy podmioty przekazujące dane zamierzają kontynuować przekazywanie, mimo że nie stwierdzono żadnych środków uzupełniających

93. EROD i EIOD przypominają, że zgodnie z poprzednimi SKU podmiot przekazujący dane musiał „przesłać" do organu nadzorczego zawiadomienie otrzymane od podmiotu odbierającego dane dotyczące niemożności przestrzegania SKU, „jeśli, pomimo otrzymania tego powiadomienia, zdecyduje się on kontynuować przekazywanie danych lub znieść jego zawieszenie". Zobowiązanie to, przeanalizowane przez TSUE w wyroku w sprawie Schrems II, pkt 145, powinno zostać zachowane w projekcie SKU.

[32] https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_pl.pdf; pkt 56.
[33] Wyrok Trybunału (wielka izba) z dnia 16 lipca 2020 r.; Data Protection Commissioner/Facebook Ireland Limited i Maximillian Schrems; sprawa C-311/18; pkt 134.
[34] https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_pl.pdf; pkt 5.

94. Zgodnie z przeanalizowanymi przez TSUE postanowieniami zawartymi w SKU z 2010 r. [35] zawiadomienie powinno mieć miejsce jedynie w przypadku, gdy podmiot przekazujący dane zamierza kontynuować przekazywanie w sytuacji braku skutecznych środków uzupełniających. Kwestii tej nie uwzględniono jeszcze w projekcie SKU, a jest to sytuacja, w której organ nadzorczy może odegrać pewną rolę i może podjąć interwencję, wykorzystując swoje uprawnienia do zawieszenia lub zakazania przekazywania danych w przypadkach, w których stwierdzi, że nie można zapewnić merytorycznie równoważnego poziomu ochrony zgodnie z wyrokiem w sprawie Schrems II[36].

95. Ponadto z brzmienia klauzuli 2 lit. f) powinno jasno wynikać, że takie zawiadomienie w żaden sposób nie będzie stanowiło zezwolenia na podstawie projektu SKU na kontynuowanie przekazywania w przypadku braku odpowiednich środków uzupełniających. EROD i EIOD wzywają zatem Komisję do jasnego sformułowania tej klauzuli.

4.3.7 Klauzula 3 – Obowiązki podmiotu odbierającego dane w przypadku wniosków administracji rządowej o dostęp

96. EROD i EIOD zalecają przedstawienie wyjaśnienia, że wnioski o dostęp pochodzące od sądów i innych organów publicznych państwa trzeciego wchodzą w zakres zastosowania tego postanowienia. Można to osiągnąć na przykład przez zmianę tytułu tej klauzuli.

4.3.7.1 Klauzula 3 akapit pierwszy – Zawiadomienie

97. Jeżeli chodzi o klauzulę 3 akapit pierwszy, EROD i EIOD podkreślają, że należy wyjaśnić, iż zawiadomienie, które podmiot odbierający dane ma złożyć, powinno zostać przesłane przed udzieleniem odpowiedzi na wniosek o dostęp złożony przez organy publiczne państwa trzeciego, tak aby umożliwić podmiotowi przekazującemu dane podjęcie w razie potrzeby wszelkich odpowiednich dalszych kroków.

4.3.7.2 Klauzula 3 akapit drugi – Kontrola legalności i minimalizacji danych

98. EROD i EIOD rozumieją, że zakres zastosowania klauzuli 3 akapit drugi jest ograniczony do sytuacji, w których wnioski o dostęp otrzymane przez podmiot odbierający dane nie będą zgodne z przepisami państwa trzeciego, w tym z jego zobowiązaniami wynikającymi z prawa międzynarodowego i jego normami kolizyjnymi. W związku z tym EROD i EIOD zalecają przedstawienie wyjaśnienia tej klauzuli celem zapewnienia, aby podmioty przekazujące dane nie zrozumiały jej błędnie. Klauzula ta ma na celu jedynie zapewnienie, aby przepisy państwa trzeciego, które spełnia już wymogi przewidziane w prawie Unii, były prawidłowo stosowane w tym państwie trzecim. W związku z tym klauzula ta nie będzie sama w sobie prowadzić do zakwestionowania legalności wniosków o ujawnienie danych pod kątem zgodności z unijnymi wymogami ochrony danych, chyba że przepisy państwa trzeciego wyraźnie przewidują możliwość powołania się na przepisy innego państwa.

[35] 2010/87/: Decyzja Komisji z dnia 5 lutego 2010 r. w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych podmiotom przetwarzającym dane mającym siedzibę w krajach trzecich na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady; Dz.U. L 39 z 12.2.2010, s. 5. Załącznik – Klauzula 4 lit. g).

[36] Wyrok Trybunału (wielka izba) z dnia 16 lipca 2020 r.; Data Protection Commissioner/Facebook Ireland Limited i Maximillian Schrems; sprawa C-311/18; pkt 113 i 121.

4.3.8 Klauzula 5 – Prawa osób, których dane dotyczą – moduł pierwszy (Przekazywanie między administratorami)

- **Klauzula 5 lit. a)**

99. Zgodnie z tą literą podmiot odbierający dane jest odpowiedzialny za rozpatrywanie żądań osób, których dane dotyczą, dotyczących wykonania przysługujących im praw. W praktyce mogą pojawić się ewentualne trudności związane z tym, że podmiot odbierający dane znajduje się poza UE. Z tego powodu EROD i EIOD podzielają opinię, zgodnie z którą klauzulę tę należy ściślej dostosować do aktualnych wymogów przewidzianych w SKU z 2004 r., tj. podmiot przekazujący dane ponosi odpowiedzialność za odpowiadanie na zapytania osób, których dane dotyczą, chyba że strony uzgodniły inaczej[37]. Dodatkowo strony powinny zobowiązać się do udzielania sobie wzajemnej pomocy i współpracowania ze sobą przy rozpatrywaniu żądań osób, których dane dotyczą.

100. Ponadto EROD i EIOD są zdania, że nałożony na podmiot odbierający dane obowiązek udzielenia informacji osobom, których dane dotyczą, na ich żądanie należy wyraźnie wprowadzić do projektu SKU oraz w pełni dostosować do wymogów określonych w art. 12 ust. 1 i art. 15 RODO.

- **Klauzula 5 lit. b)**

101. Zdaniem EROD i EIOD osobom, których dane dotyczą, powinno przysługiwać prawo do uzyskania dostępu – na żądanie – do większej ilości informacji niż informacje aktualnie wymienione w klauzuli 5 lit. b) ppkt (i), a ściślej mówiąc do:

- bardziej szczegółowych informacji związanych z dalszym przekazaniem danych, w tym podwykonawcom przetwarzania, tj. imienia i nazwiska oraz danych kontaktowych wszystkich odbiorców związanych z nimi danych[38]. Powyższe można osiągnąć, wprowadzając wymóg, aby strony przekazywały takie informacje w załączniku III do projektu SKU, lub wymóg, aby strony przekazywały te informacje osobom, których dane dotyczą, na ich żądanie;
- szczegółowych informacji na temat planowanego okresu przechowywania danych osobowych, gdy jest to możliwe, a gdy nie jest to możliwe – kryteriów ustalania tego okresu, zgodnie z art. 15 ust. 1 lit. d) RODO. Powyższe można osiągnąć, wprowadzając wymóg, aby strony przekazywały takie informacje w załączniku I do projektu SKU. Przekazywanie takich informacji w załączniku I może również uświadomić stronom, że mają one obowiązek faktycznego określenia i wdrożenia okresów zatrzymywania; oraz
- jeżeli dane osobowe nie zostały zebrane bezpośrednio od osób, których dane dotyczą – wszelkich dostępnych informacji o ich źródle zgodnie z art. 15 ust. 1 lit. g) RODO.

102. Moduł pierwszy powinien obejmować spoczywający na podmiocie odbierającym dane obowiązek poinformowania osób, których dane dotyczą, o przysługujących im prawach do żądania sprostowania lub usunięcia ich danych osobowych, a także przysługujących im prawach do żądania ograniczenia przetwarzania ich danych osobowych lub wniesienia sprzeciwu wobec ich przetwarzania, co prowadziłoby do dostosowania tej klauzuli do przepisów art. 15 ust. 1 lit. e) RODO. Informacje takie stanowiłyby uzupełnienie informacji o prawie wniesienia skargi do właściwego organu nadzorczego uwzględnionych obecnie w klauzuli 5 lit. b) ppkt (i). Ogólnie rzecz biorąc, EROD i EIOD wzywają Komisję

[37] Zob. klauzula 1 lit. d) i klauzula II lit. e) w SKU z 2004 r.

[38] Zob. wyrok Trybunału (trzecia izba) z dnia 7 maja 2009 r.; TSUE, College van burgemeester en wethouders van Rotterdam/M.E.E. Rijkeboer, C-553/07; pkt 49 i 54.

do wprowadzenia przepisu zobowiązującego podmiot odbierający dane do umożliwienia osobom, których dane dotyczą, wykonania przysługującego im prawa do żądania ograniczenia przetwarzania dotyczących ich danych.

103. Jeżeli chodzi o klauzulę 5 lit. b) ppkt (iii) dotyczącą usunięcia danych osobowych osób, których dane dotyczą, EROD i EIOD są zdania, że tego rodzaju zobowiązanie powinno w pełni odzwierciedlać wymogi określone w art. 17 ust. 1 RODO.

- **Klauzula 5 lit. c)**

104. EROD i EIOD uważają, że ograniczenie prawa do wniesienia sprzeciwu do przypadków marketingu bezpośredniego jest nieuzasadnione oraz że zakres prawa do wniesienia sprzeciwu należy rozszerzyć, w szczególności w przypadkach, w których prawo to jest wykonalne w pierwszej kolejności względem podmiotu przekazującego dane.

- **Klauzula 5 lit. d)**

105. Zdaniem EROD i EIOD brzmienie klauzuli 5 lit. d) powinno zostać zmienione, tak aby odzwierciedlało przewidziany w art. 22 RODO zakaz zautomatyzowanego podejmowania decyzji stanowiący zasadę ogólną, oraz powinno określać warunki dopuszczające odstępstwa od tego zakazu. W klauzuli 5 lit. d) należy również wyjaśnić, że spoczywające na podmiocie odbierającym dane obowiązki wdrożenia odpowiednich zabezpieczeń i przekazywania osobom, których dane dotyczą, informacji o planowanym zautomatyzowanym podjęciu decyzji mają charakter łączny.

106. Ponadto zgodnie z art. 22 i art. 15 ust. 1 lit. h) RODO klauzula 5 lit. d) powinna zawierać wymóg, zgodnie z którym informacje przekazywane osobom, których dane dotyczą, powinny obejmować znaczenie i przewidywane konsekwencje przetwarzania dla tych osób.

- **Klauzula 5 lit. f)**

107. Mimo iż EROD i EIOD przyznają, że mogą zaistnieć okoliczności uzasadniające odmowę podjęcia działań na żądanie osoby, której dane dotyczą, przez podmiot odbierający dane, w projekcie SKU należy wyraźnie podkreślić, że w klauzuli tej należy uwzględnić wyłącznie wymogi przewidziane w przepisach lokalnych nienaruszające istoty podstawowych praw i wolności oraz niewykraczające poza to, co jest konieczne i proporcjonalne w społeczeństwie demokratycznym do osiągnięcia jednego z celów wymienionych w art. 23 ust. 1 RODO.

- **Klauzula 5 lit. g)**

108. EROD i EIOD uważają, że aby zapewnić osobom, których dane dotyczą, pełną możliwość wykonywania przysługujących im praw, obowiązek informowania osób, których dane dotyczą, o tym, że podmiot odbierający dane zamierza odrzucić ich żądanie, należy dostosować do przepisów art. 12 ust. 4 RODO, a zatem taką informację należy przekazać niezwłocznie i nie później niż w terminie jednego miesiąca od otrzymania żądania.

4.3.9 Klauzula 5 – Prawa osób, których dane dotyczą – moduły drugi (Przekazywanie przez administratora podmiotowi przetwarzającemu) i trzeci (Przekazywanie między podmiotami przetwarzającymi)

109. Klauzula 5 w module drugim i klauzula 5 w module trzecim zawierają te same wymogi, wobec czego w niniejszej wspólnej opinii omawia się je łącznie.

110. EROD i EIOD podzielają zdanie, zgodnie z którym w klauzuli 5 lit. a) należy:

- doprecyzować, że odpowiedzi osobom, których dane dotyczą, udziela się zgodnie z instrukcjami administratora (np. dotyczącymi treści odpowiedzi), jak określono w załączniku do projektu SKU;
- doprecyzować, że zakres spoczywającego na podmiocie odbierającym dane obowiązku dotyczącego wykonywania praw osób, których dane dotyczą, w imieniu administratora powinien być opisany i wyraźnie określony w załączniku do projektu SKU.

4.3.10 Klauzula 5 – Prawa osób, których dane dotyczą – moduł czwarty (Przekazywanie przez podmiot przetwarzający administratorowi)

111. EROD i EIOD z zadowoleniem przyjęliby wyjaśnienia ze strony Komisji Europejskiej dotyczące możliwych praktycznych konsekwencji podjętego przez strony zobowiązania polegającego na udzielaniu sobie wzajemnej pomocy przy rozpatrywaniu żądań osób, których dane dotyczą, zgłoszonych na podstawie mających zastosowanie przepisów prawa podmiotu odbierającego dane.

112. EROD i EIOD z zadowoleniem przyjęliby dalsze wyjaśnienia dotyczące sytuacji, które obejmować ma podjęte przez strony zobowiązanie polegające na udzielaniu sobie wzajemnej pomocy przy rozpatrywaniu żądań osób, których dane dotyczą.

113. Ponadto niejasne pozostaje zamierzone znaczenie klauzuli 5, w której odniesiono się do pomocy „na potrzeby przetwarzania danych przez podmiot przekazujący dane w UE na podstawie RODO". Jeżeli zamierzano na przykład uwzględnić pomoc związaną z obowiązkami z zakresu bezpieczeństwa, Komisja powinna doprecyzować tę kwestię w projekcie SKU.

4.3.11 Klauzula 6 – Środki zaskarżenia

114. EROD i EIOD z zadowoleniem przyjęliby wyjaśnienie w projekcie SKU, czy wariant zakładający oferowanie osobom, których dane dotyczą, możliwości nieodpłatnego wniesienia środka zaskarżenia do niezależnego organu rozstrzygania sporów należy przewidzieć we wszystkich zestawach klauzul. Mimo iż byłoby jasne, że wariant ten może przyczynić się do zapewnienia skutecznego egzekwowania przepisów w przypadku przekazywania danych między administratorami, EROD i EIOD z zadowoleniem przyjęliby dalsze wyjaśnienia dotyczące tego, w jaki sposób mechanizm ten będzie stosowany w modułach drugim, trzecim i czwartym. Na przykład należy wyjaśnić, w jakim zakresie mechanizm ten miałby zastosowanie w związku ze szczególnymi i bezpośrednimi obowiązkami podmiotu przetwarzającego i administratora w module czwartym.

115. Jeżeli chodzi o klauzule dotyczące środków zaskarżenia przewidziane w modułach pierwszym, drugim i trzecim (klauzula 6 lit. b)), EROD i EIOD są zdania, że należy doprecyzować, iż podmiot odbierający dane uznaje przysługujące osobie, której dane dotyczą (która powołuje się na swoje prawa jako beneficjent będący osobą trzecią), prawo do bezpośredniego wniesienia skargi do organu nadzorczego w EOG lub wytoczenia powództwa przed sąd w EOG bez konieczności podjęcia uprzedniej próby polubownego rozstrzygnięcia sporu. W praktyce, aby zapewnić taki sam poziom ochrony jak poziom przewidziany w art. 77 i 79 RODO, należy promować tego rodzaju mechanizmy (np. wewnętrzne mechanizmy rozpatrywania skarg wdrożone przez podmiot odbierający dane), aby ułatwić beneficjentom będącym osobami trzecimi wykonywanie ich praw, przy czym mechanizmów tych nie należy uznawać za przesłankę wniesienia skargi do organu nadzorczego lub wytoczenia powództwa przed sąd.

116. Dodatkowo art. 77 ust. 1 RODO przewiduje, że osoby, których dane dotyczą, mogą zdecydować o wniesieniu skargi do organu nadzorczego w miejscu swojego zwykłego pobytu, w swoim miejscu pracy lub w miejscu popełnienia domniemanego naruszenia. Z tej perspektywy EROD i EIOD uznają, że istotne jest dokonanie odpowiedniej zmiany klauzuli 6 lit. b) ppkt (i), ponieważ wydaje się, iż projekt

SKU odnosi się wyłącznie do organu nadzorczego odpowiedzialnego za zapewnianie przestrzegania przez podmiot przekazujący dane przepisów RODO dotyczących przekazywania danych.

117. EROD i EIOD wzywają do wyjaśnienia braku klauzuli dotyczącej środków zaskarżenia w module czwartym. Biorąc pod uwagę zobowiązania zawarte obecnie w klauzuli 5 w module czwartym związane z „przetwarzaniem danych przez podmiot przekazujący dane w UE na podstawie RODO", EROD i EIOD zastanawiają się, w jaki sposób przysługujące osobom, których dane dotyczą, prawo do środka zaskarżenia będzie uznawane w takich przypadkach.

4.3.12 Klauzula 7 – Odpowiedzialność – moduły pierwszy (Przekazywanie między administratorami) i czwarty (Przekazywanie przez podmiot przetwarzający administratorowi)

118. Jeżeli chodzi o klauzulę 7 w modułach pierwszym i czwartym, EROD i EIOD zauważają, że do pociągnięcia do odpowiedzialności solidarnej względem osoby, której dane dotyczą, doszłoby wyłącznie w przypadku wspólnej odpowiedzialności. Inaczej mówiąc, system odpowiedzialności przedstawiony w projekcie SKU nie przewiduje odpowiedzialności solidarnej, w przypadku której każda ze stron ponosiłaby odpowiedzialność za szkodę wyrządzoną wyłącznie przez drugą stronę.

119. W tym kontekście EROD i EIOD pragną przypomnieć, że projekt SKU powinien zawierać skuteczne mechanizmy umożliwiające zapewnienie w praktyce zgodności z poziomem ochrony wymaganym prawem Unii[39]. Wytoczenie powództwa przeciwko przedsiębiorstwu spoza UE może się jednak okazać trudne dla osoby, której dane dotyczą, jeżeli chodzi o wykonanie wyroku przeciwko przedsiębiorstwu spoza UE. Jako że istniejące zestawy SKU zapewniają większą ochronę niż ochrona zaproponowana w projekcie SKU, EROD i EIOD są zdania, że ochrona osób, których dane dotyczą, powinna zostać w tym zakresie wzmocniona.

120. W tym kontekście EROD i EIOD wzywają do zmiany klauzuli 7 zgodnie z powyższymi rozważaniami.

4.3.13 Klauzula 7 – Odpowiedzialność – moduły drugi (Przekazywanie przez administratora podmiotowi przetwarzającemu) i trzeci (Przekazywanie między podmiotami przetwarzającymi)

121. W klauzuli 7 lit. c) i d) w modułach drugim i trzecim przewidziano, że osoba, której dane dotyczą, jest uprawniona do otrzymania odszkodowania za wszelkie szkody majątkowe i niemajątkowe wyrządzone przez podmiot odbierający dane od podmiotu odbierającego dane (lit. c)) lub od podmiotu przekazującego dane (lit. d)).

122. Aby uniknąć wątpliwości, w projekcie SKU Komisja powinna wyjaśnić, że możliwości te mają charakter łączny, a osoba, której dane dotyczą, może zdecydować, że otrzyma odszkodowanie za wszelkie szkody majątkowe i niemajątkowe wyrządzone przez podmiot odbierający dane albo od podmiotu odbierającego dane, albo od podmiotu przekazującego dane. Inaczej mówiąc, możliwość pociągnięcia do odpowiedzialności podmiotu przekazującego dane za wszelkie szkody majątkowe lub niemajątkowe wyrządzone przez podmiot przekazujący dane nie powinna zależeć od wytoczenia powództwa przeciwko podmiotowi odbierającemu dane.

[39] Na przykład art. 47 ust. 2 lit. f) RODO zawiera wymóg, zgodnie z którym w wiążących regułach korporacyjnych określa się między innymi „przyjęcie przez administratora lub podmiot przetwarzający posiadających jednostki organizacyjne na terytorium państwa członkowskiego odpowiedzialności prawnej za naruszenie wiążących reguł korporacyjnych przez odnośnego członka niemającego jednostki organizacyjnej w Unii".

4.3.14 Klauzula 9 – Nadzór

123. W klauzuli 9 przewidziano wymóg określenia organu nadzorczego właściwego dla podmiotu przekazującego dane na potrzeby zapewnienia zgodności z projektem SKU, lecz nie przewidziano przypadku, w którym może występować kilka właściwych organów nadzorczych, jeżeli występuje kilka podmiotów przekazujących dane będących stronami projektu SKU (co jest jedną z możliwości oferowanych w projekcie SKU). EROD i EIOD zalecaliby wyjaśnienie tej kwestii przez odniesienie się do możliwości, w której właściwy mógłby być więcej niż jeden organ nadzorczy w EOG, jeżeli zaangażowane są różne podmioty przekazujące dane, oraz w której – w tym konkretnym przypadku – każdy organ nadzorczy odpowiedzialny za zapewnienie zgodności przez podmiot przekazujący dane będzie właściwy dla konkretnej czynności przekazywania danych przeprowadzonej na jego terytorium. Mając na względzie jasność i czytelność, należy wezwać strony do wskazania właściwych organów nadzorczych w załącznikach.

4.4 Sekcja III - Postanowienia końcowe

4.4.1 Klauzula 1 – Brak zgodności z klauzulami i rozwiązanie umowy

124. W klauzuli 1 lit. d) przewidziano wyjątek od obowiązku zwrotu lub usunięcia danych przed rozwiązaniem umowy, gdy przepisy lokalne mające zastosowanie do podmiotu odbierającego dane zakazują takiego zwrotu lub usunięcia. EROD i EIOD wzywają Komisję do przypomnienia, że obowiązki spoczywające na podmiocie odbierającym dane na mocy klauzuli 5 w sekcji II miałyby zastosowanie również w przypadku, o którym mowa w klauzuli 1 lit. d) w sekcji III. EROD i EIOD uważają, że Komisja powinna wyjaśnić w projekcie SKU, że w klauzuli tej należy uwzględnić wyłącznie wymogi przewidziane w przepisach lokalnych nienaruszające istoty podstawowych praw i wolności oraz niewykraczające poza to, co jest konieczne i proporcjonalne w społeczeństwie demokratycznym do osiągnięcia jednego z celów wymienionych w art. 23 ust. 1 RODO.

125. Dodatkowo EROD i EIOD zauważają, że klauzula 1 lit. d) przewiduje, że podmiot odbierający dane powinien zagwarantować, że zapewni „w możliwym zakresie" poziom ochrony wymagany w tych klauzulach.

126. W tym zakresie EROD i EIOD przypominają, że poziom ochrony wymagany w projekcie SKU powinien być zawsze zapewniony. EROD i EIOD wzywają zatem Komisję do usunięcia wyrażenia „w możliwym zakresie".

4.5 Załączniki

127. EROD i EIOD zauważają, że projekt SKU stworzono z myślą o jego możliwym wykorzystaniu – jako umowy wielostronnej – przez więcej niż jedną stronę będącą podmiotem przekazującym dane lub podmiotem odbierającym dane. W celu uniknięcia ryzyka związanego z zacieraniem się ról i obowiązków ważne jest, aby w projekcie SKU strony uzyskały jasne wskazówki dotyczące odpowiedniego wypełnienia załącznika. Jest to tym bardziej niezbędne ze względu na podejście modułowe umożliwiające włączenie klauzul do jednej umowy wielostronnej obejmującej maksymalnie cztery scenariusze (przekazywanie między administratorami, przez administratora podmiotowi przetwarzającemu, między podmiotami przetwarzającymi oraz przez podmiot przetwarzający administratorowi) i prawdopodobnie dużą liczbę czynności przekazywania, z których w każdej mogą uczestniczyć różne podmioty przekazujące dane lub podmioty odbierające dane. EROD i EIOD uważają zatem, że niezwykle istotne jest, aby w umowie, która zostanie podpisana w praktyce, łącznie z załącznikami, określono w sposób całkowicie przejrzysty role i obowiązki każdej ze stron (podmiot przekazujący dane – administrator, podmiot przekazujący dane – podmiot przetwarzający, podmiot odbierający dane – administrator, podmiot odbierający dane – podmiot przetwarzający) w każdej relacji i w odniesieniu do każdego jednorazowego lub wielokrotnego przekazania objętego umową.

128. Z tych powodów załącznik do umowy powinien być dostatecznie precyzyjny, aby w dowolnym momencie możliwe było określenie, kto odgrywa jaką rolę w przypadku konkretnego jednorazowego lub wielokrotnego przekazania danych osobowych. EROD i EIOD zalecają zatem wyjaśnienie, że **każde jednorazowe lub wielokrotne przekazywanie**, tj. każde jednorazowe lub wielokrotne przekazanie przeprowadzone w co najmniej jednym określonym i zdefiniowanym celu, należy odrębnie opisać na podstawie jego celu lub celów, rodzajów przekazywanych danych osobowych, kategorii osób, których dane dotyczą, rodzaju lub rodzajów przetwarzania oraz stron czynności przekazywania (podmiot odbierający dane/podmioty odbierające dane i podmiot przekazujący dane/podmioty przekazujące dane), a także roli odpowiednich stron (administrator/administratorzy lub podmiot przetwarzający/podmioty przetwarzające). W rezultacie co do zasady zawsze wymagany będzie odrębny załącznik, który powinien zawierać części I–VI, dla każdego jednorazowego lub wielokrotnego przekazania. Taki odrębny załącznik wymagany dla każdego jednorazowego lub wielokrotnego przekazania powinien zostać podpisany wyłącznie przez te podmioty przekazujące dane i podmioty odbierające dane, które dokonują odpowiedniego przekazania. Jednocześnie w celu uniknięcia dwuznaczności każdy podmiot przekazujący dane i podmiot odbierający dane podpisujący odpowiedni załącznik powinien określić – przy podpisywaniu załącznika związanego z odpowiednim jednorazowym lub wielokrotnym przekazaniem – swoją rolę w przypadku tego jednorazowego lub wielokrotnego przekazania (administrator lub podmiot przetwarzający).

129. W rezultacie w przypadku umowy wielostronnej dotyczącej kilku czynności przekazania lub obejmującej kilka stron zawsze należy doprecyzować, który załącznik (zawierający części I–VI) dotyczy którego konkretnego jednorazowego lub wielokrotnego przekazania, kim są podmioty przekazujące dane i podmioty odbierające dane zaangażowane w takie jednorazowe lub wielokrotne przekazanie oraz jaką rolę (administratora lub podmiotu przetwarzającego) odgrywa odpowiedni podmiot przekazujący dane lub podmiot odbierający dane w takim jednorazowym lub wielokrotnym przekazaniu. W tym celu EROD i EIOD sugerują uwzględnienie jakiegoś rodzaju wyjaśnienia w części projektu SKU poświęconej załącznikom mającego na celu wskazanie stronom właściwego stosowania i podpisania załącznika, w szczególności w przypadku projektu SKU wykorzystywanego jako umowa wielostronna. W załączniku technicznym do niniejszej wspólnej opinii EROD i EIOD przedstawili pewne odpowiadające propozycje takich sformułowań.

130. Wobec powyższego załącznika zawierającego wyłącznie ogólne informacje mające zastosowanie do szeregu czynności przekazywania nie należy uznawać za kompletny. Aby uniknąć pomyłek, załącznik powinny podpisać wyłącznie strony, które faktycznie dokonują konkretnego przetwarzania, w tym strony przystępujące do klauzul na podstawie sekcji I klauzula 6.

131. Innym problemem napotykanym w praktyce jest fakt, że załączniki do SKU dotyczące środków technicznych i organizacyjnych często wypełnia się w sposób bardzo ogólny, ponieważ mają one odpowiadać całemu szeregowi różnych czynności przekazywania i przetwarzania, a jednocześnie brakuje w nich precyzyjnych wskazówek dotyczących tego, które środki techniczne i organizacyjne należy zastosować w przypadku poszczególnych czynności przekazywania objętych SKU. EROD i EIOD sugerują zatem, aby w projekcie SKU (część III załącznika zgodnie z sugestią EROD i EIOD) wyraźnie podkreślić, że wymienić należy wyłącznie te szczególne środki techniczne i organizacyjne, które będą stosowane w przypadku odpowiedniego jednorazowego lub wielokrotnego przekazania, natomiast środki techniczne i organizacyjne, które będą mieć zastosowanie wyłącznie do innych czynności/kategorii czynności przekazania objętych tą samą umową wielostronną, należy podać wyłącznie w załączniku dotyczącym tych odpowiednich czynności przekazania.

132. Jeżeli chodzi o relacje administrator – podmiot przetwarzający, EROD i EIOD zauważają, że w praktyce czasami dochodzi do nieporozumień dotyczących wymogów związanych z podwykonawcami przetwarzania. W części V załącznika należy wyraźnie przypomnieć i odzwierciedlić określone w projekcie SKU wymogi dotyczące wymienienia każdego podwykonawcy przetwarzania. Ponadto EROD i EIOD zalecaliby wskazanie (jak zasugerowano, w części V załącznika) wykazu zamierzonych

podwykonawców przetwarzania (w tym – w odniesieniu do każdego z nich – ich lokalizacji, czynności przetwarzania oraz rodzaju wdrożonych przez nich zabezpieczeń), aby umożliwić administratorowi wyrażenie zgody na korzystanie z usług zamierzonych podwykonawców przetwarzania zgodnie z wymogami określonymi w art. 28 ust. 2 RODO. Ponadto przydatne byłoby również włączenie zdania oznajmującego, że administrator wyraził zgodę na korzystanie z usług podwykonawców przetwarzania wymienionych w tym wykazie.

W imieniu Europejskiej Rady Ochrony Danych	W imieniu Europejskiej Rady Ochrony Danych
Europejski Inspektor Ochrony Danych	Przewodnicząca
(Wojciech Wiewiórowski)	(Andrea Jelinek)



Translations proofread by EDPB Members.
This language version has not yet been proofread.

SPIS TREŚCI

1 Kontekst 3
2 Zakres opinii 4
3 Ogólne uzasadnienie dotyczące projektu decyzji i projektu standardowych klauzul umownych 4
3.1 Uwagi ogólne 4
3.2 Wyjaśnienie zastosowanej metodyki i struktury dokumentu 5
4 Analiza projektu decyzji i załącznika do tej decyzji 6
4.1 Główne uwagi dotyczące projektu decyzji 6
4.1.1 Uwagi dotyczące zakresu stosowania decyzji i powiązania z innym zbiorem projektów standardowych klauzul umownych w sprawie przekazywania danych 6
4.2 Główne uwagi dotyczące załącznika do decyzji wykonawczej Komisji 7
4.2.1 Cel i zakres (klauzula 1 w projekcie standardowych klauzul umownych) 7
4.2.2 Niezmienność (klauzula 2 w projekcie standardowych klauzul umownych) 7
4.2.3 Klauzula przystąpienia (klauzula 5 w projekcie standardowych klauzul umownych) 8
4.2.4 Obowiązki stron (klauzula 7 w projekcie standardowych klauzul umownych) 8
4.2.5 Prawa osoby, której dane dotyczą (klauzula 8 w projekcie standardowych klauzul umownych) 10
4.2.6 Załączniki do projektu standardowych klauzul umownych 11

Europejska Rada Ochrony Danych i Europejski Inspektor Ochrony Danych

uwzględniając art. 42 ust. 2 rozporządzenia (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE („**rozporządzenie (UE) 2018/1725**"),

uwzględniając Porozumienie EOG, w szczególności załącznik XI i protokół 37 do tego Porozumienia, zmienione decyzją Wspólnego Komitetu EOG nr 154/2018 z dnia 6 lipca 2018 r.[1],

PRZYJMUJĄ NINIEJSZĄ WSPÓLNĄ OPINIĘ

1 KONTEKST

1. W kontekście stosunków umownych między administratorem a podmiotem przetwarzającym lub podmiotami przetwarzającymi w celu przetwarzania danych osobowych, w art. 28 rozporządzenia (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych lub „**RODO**") ustanowiono zestaw przepisów dotyczących zawarcia konkretnej umowy między zaangażowanymi stronami oraz przepisów, które należy do niej włączyć obowiązkowo.

2. Zgodnie z art. 28 ust. 3 RODO przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy lub innego instrumentu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i administratora, określając zbiór konkretnych aspektów regulujących stosunek umowny między stronami. Obejmują one m.in. przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą. W art. 28 ust. 4 przewidziano dodatkowe wymogi, jeżeli do wykonania w imieniu administratora konkretnych czynności przetwarzania podmiot przetwarzający korzysta z usług innego podmiotu przetwarzającego.

3. Na mocy art. 28 ust. 6 RODO, bez uszczerbku dla indywidualnych umów między administratorem a podmiotem przetwarzającym, umowa lub inny akt prawny, o których mowa w art. 28 ust. 3 i 4 RODO, mogą się opierać w całości lub w części na standardowych klauzulach umownych. Przedmiotowe standardowe klauzule umowne mają zostać przyjęte w odniesieniu do kwestii, o których mowa w ust. 3 i 4.

4. Art. 28 ust. 7 RODO stanowi, że Komisja może określić standardowe klauzule umowne dotyczące kwestii, o których mowa w ust. 3 i 4 niniejszego artykułu, zgodnie z procedurą sprawdzającą, o której mowa w art. 93 ust. 2.

5. W rozporządzeniu (UE) 2018/1725 ustanawia się przepisy o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy Unii oraz przepisy o swobodnym przepływie danych osobowych między nimi lub do odbiorców mających siedzibę w Unii.

[1] Odniesienia do „państw członkowskich" zawarte w niniejszej opinii należy rozumieć jako odniesienia do „państw należących do EOG".

6. Art. 29 ust. 3, 4 i 7 rozporządzenia (UE) 2018/1725 zawiera wymogi podobne do tych zawartych w art. 28 ust. 3, 4 i 7 RODO. Jest to uzasadnione faktem, że w interesie spójnego podejścia do ochrony danych osobowych w całej Unii oraz swobodnego przepływu danych osobowych w Unii przepisy o ochronie danych mające zastosowanie do sektora publicznego w państwach członkowskich dostosowano w jak największym stopniu do przepisów o ochronie danych dotyczących instytucji, organów i jednostek organizacyjnych Unii.

2 ZAKRES OPINII

7. W dniu 12 listopada 2020 r. Komisja opublikowała:

   - projekt decyzji wykonawczej Komisji w sprawie standardowych klauzul umownych między administratorami a podmiotami przetwarzającymi dotyczących kwestii, o których mowa w art. 28 ust. 3 i 4 rozporządzenia (UE) 2016/679 oraz art. 29 ust. 7 rozporządzenia (UE) 2018/1725) („**projekt decyzji**");
   - projekt załącznika do decyzji wykonawczej Komisji w sprawie standardowych klauzul umownych między administratorami a podmiotami przetwarzającymi dotyczących kwestii, o których mowa w art. 28 ust. 3 i 4 rozporządzenia (UE) 2016/679 oraz art. 29 ust. 7 rozporządzenia (UE) 2018/1725) („**projekt standardowych klauzul umownych**").

8. Tego samego dnia Komisja Europejska opublikowała również projekt swojej decyzji wykonawczej wraz z załącznikiem w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich zgodnie z rozporządzeniem (UE) 2016/679.

9. W dniu 12 listopada 2020 r. Komisja Europejska zwróciła się do Europejskiej Rady Ochrony Danych (EROD) i Europejskiego Inspektora Ochrony Danych (EIOD) o wydanie wspólnej opinii na podstawie art. 42 ust. 1 i 2 rozporządzenia (UE) 2018/1725 w sprawie tych dwóch zbiorów projektów standardowych klauzul umownych i odpowiednich aktów wykonawczych.

10. W celu zapewnienia jasności EROD i EIOD postanowili wydać dwie odrębne opinie w sprawie tych dwóch zbiorów standardowych klauzul umownych.

11. Zakres niniejszej opinii ogranicza się zatem do projektu decyzji i projektu standardowych klauzul umownych między administratorami a podmiotami przetwarzającymi dotyczących kwestii, o których mowa w art. 28 ust. 3 i 4 RODO oraz art. 29 ust. 3 i 4 rozporządzenia (UE) 2018/1725.

3 OGÓLNE UZASADNIENIE DOTYCZĄCE PROJEKTU DECYZJI I PROJEKTU STANDARDOWYCH KLAUZUL UMOWNYCH

3.1 Uwagi ogólne

12. Każdy zbiór standardowych klauzul umownych musi dodatkowo określać przepisy przewidziane w art. 28 RODO i art. 29 rozporządzenia (UE) 2018/1725. Opinia EROD i EIOD ma na celu zapewnienie spójności i prawidłowego stosowania art. 28 RODO w odniesieniu do przedstawionego projektu standardowych klauzul umownych, które mogłyby służyć jako standardowe klauzule umowne zgodnie z art. 28 ust. 7 RODO i art. 29 ust. 7 rozporządzenia (UE) 2018/1725.

13. EROD i EIOD są zdania, że klauzule będące jedynie powtórzeniem przepisów art. 28 ust. 3 i 4 RODO oraz art. 29 ust. 3 i 4 rozporządzenia (UE) 2018/1725 nie są odpowiednie do tego, by stanowić standardowe klauzule umowne. Rada i EIOD postanowili zatem przeanalizować ten dokument w całości, wraz z załącznikami. Zdaniem Rady i EIOD w umowie na mocy art. 28 RODO lub art. 29 rozporządzenia (UE) 2018/1725 należy dokładniej określić i wyjaśnić, w jaki sposób przepisy te zostaną spełnione. Właśnie w tym świetle analizuje się projekty standardowych klauzul umownych przedłożone Radzie i EIOD do zaopiniowania.

14. Przyjęte standardowe klauzule umowne stanowią zestaw gwarancji, które należy stosować w obecnej formie, ponieważ mają one na celu ochronę osób, których dane dotyczą, oraz ograniczenie szczególnych ryzyk związanych z podstawowymi zasadami ochrony danych.

15. EROD i EIOD zasadniczo z zadowoleniem przyjmują przyjęcie standardowych klauzul umownych jako silnego narzędzia rozliczalności, które ułatwia administratorom i podmiotom przetwarzającym przestrzeganie ich obowiązków wynikających z RODO i rozporządzenia (UE) 2018/1725.

16. EROD wydała już opinie w sprawie standardowych klauzul umownych przygotowanych przez duński[2] i słoweński organ nadzorczy[3].

17. Aby zapewnić spójne podejście do ochrony danych osobowych w całej Unii, EROD i EIOD z dużym zadowoleniem przyjmują planowane przyjęcie przez Komisję standardowych klauzul umownych o skutku ogólnounijnym.

18. Ten sam zbiór standardowych klauzul umownych będzie faktycznie miał zastosowanie niezależnie od tego, czy ten stosunek umowny dotyczy podmiotów prywatnych, organów publicznych państw członkowskich czy instytucji lub organów UE. Takie obowiązujące w całej UE standardowe klauzule umowne zapewnią dalszą harmonizację i pewność prawa.

19. EROD i EIOD również z zadowoleniem przyjmują fakt, że ten sam zbiór standardowych klauzul umownych powinien mieć zastosowanie w odniesieniu do stosunków umownych między administratorami a podmiotami przetwarzającymi, podlegającymi odpowiednio RODO i rozporządzeniu (UE) 2018/1725.

3.2 Wyjaśnienie zastosowanej metodyki i struktury dokumentu

20. W celu zachowania przejrzystości niniejsza opinia składa się z (i) części zasadniczej, w której wyszczególniono uwagi ogólne, jakie pragną przedstawić EROD i EIOD, oraz (ii) załącznika, w którym przedstawiono uwagi o charakterze bardziej technicznym dotyczące bezpośrednio projektu decyzji i projektu standardowych klauzul umownych w celu podania kilku przykładów ewentualnych zmian. Między uwagami ogólnymi i technicznymi nie obowiązuje żadna hierarchia.

21. Ponadto główne uwagi dotyczące projektu decyzji i projektu standardowych klauzul umownych przedstawiono w dwóch oddzielnych sekcjach. W razie potrzeby, w celu zapewnienia spójności, zamieszczono odesłania.

[2] Opinia 14/2019 w sprawie projektu standardowych klauzul umownych przedłożonego przez duński organ nadzorczy (art. 28 ust. 8 RODO): https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinion_201914_dk_scc_pl.pdf.
[3] Opinia 17/2020 w sprawie projektu standardowych klauzul umownych przedłożonego przez organ nadzorczy Słowenii (art. 28 ust. 8 RODO): https://edpb.europa.eu/our-work-tools/our-documents/opinjoni-tal-bord-art-64/opinion-172020-draft-standard-contractual_pl.

22. Dla zachowania spójności, w stosownych przypadkach, podano również odesłania do wspólnej opinii 02/2021 EROD i EIOD w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich.

4 ANALIZA PROJEKTU DECYZJI I ZAŁĄCZNIKA DO TEJ DECYZJI

4.1 Główne uwagi dotyczące projektu decyzji

4.1.1 Uwagi dotyczące zakresu stosowania decyzji i powiązania z innym zbiorem projektów standardowych klauzul umownych w sprawie przekazywania danych

23. Art. 2 projektu decyzji stanowi, że „standardowe klauzule umowne określone w załączniku można stosować w umowach zawieranych między administratorem a podmiotem przetwarzającym, który przetwarza dane osobowe w jego imieniu, w przypadku gdy administrator i podmiot przetwarzający podlegają rozporządzeniu (UE) 2016/679 lub rozporządzeniu (UE) 2018/1725".

24. EROD i EIOD są zdania, że obecne brzmienie tego artykułu jest źródłem braku pewności prawa co do sytuacji, w których podmioty będą mogły powoływać się na przedmiotowe standardowe klauzule umowne.

25. EROD i EIOD rozumieją, że intencją Komisji jest, aby przedmiotowe standardowe klauzule umowne dotyczyły wyłącznie sytuacji wewnątrzunijnych, oraz że nie należy opierać się na tych klauzulach w przypadku przekazywania danych w rozumieniu rozdziału V. W takich przypadkach strony powinny raczej opierać się na odrębnym zbiorze standardowych klauzul umownych, który ustanowiono na potrzeby przekazywania danych osobowych do państw trzecich zgodnie z rozporządzeniem (UE) 2016/679 i który ma również obejmować wymogi określone w art. 28 ust. 3 i 4 RODO („**standardowe klauzule umowne w sprawie przekazywania danych**").

26. EROD i EIOD uważają, że projekt decyzji nie zapewnia stronom wystarczającej jasności, a dokładny zakres decyzji musi zostać jasno określony i wyszczególniony w konkretnym motywie projektu decyzji, np. przed obecnym motywem 10 projektu decyzji.

27. Ponadto Rada i EIOD są zdania, że obecne brzmienie art. 2 projektu decyzji nie ogranicza zakresu stosowania do sytuacji wewnątrzunijnych, ponieważ administratorzy lub podmioty przetwarzające podlegający RODO w odniesieniu do danej czynności przetwarzania mogą mieć siedzibę poza UE na mocy art. 3 ust. 2 RODO. Należy wówczas wyjaśnić, czy w tej sytuacji można powoływać się na przedmiotowe standardowe klauzule umowne.

28. EROD i EIOD są raczej zdania, że zamierzone ograniczenie do sytuacji wewnątrzunijnych nie jest uzasadnione. Na przykład EROD i EIOD nie widzą powodu, aby uniemożliwiać podmiotom powoływanie się na przedmiotowe standardowe klauzule umowne – w celu zapewnienia zgodności z art. 28 ust. 3 i 4 RODO – jeżeli jedna ze stron nie podlega RODO w odniesieniu do danej czynności przetwarzania, ale ma siedzibę w odpowiednim państwie. Jeżeli zakres stosowania standardowych klauzul umownych zostanie rozszerzony na sytuacje obejmujące przekazywanie danych poza UE, należy wyjaśnić stronom, że przedmiotowe standardowe klauzule umowne zapewnią zgodność z wymogami określonymi w art. 28 ust. 3 i 4 RODO lub art. 29 ust. 3 i 4 rozporządzenia (UE) 2018/1725, ale nie ze wszystkimi wymogami wynikającymi z RODO lub rozporządzenia (UE) 2018/1725, np. wymogami dotyczącymi zasad związanych z międzynarodowym przekazywaniem danych.

29. Zdaniem EROD i EIOD ważne jest również, aby w decyzji jasno wyjaśnić powiązanie i zależność między przedmiotowym zbiorem standardowych klauzul umownych a standardowymi klauzulami umownymi w sprawie przekazywania danych. Należy wyjaśnić stronom – już w decyzji – że jeżeli zamierzają skorzystać ze standardowych klauzul umownych zarówno na mocy art. 28 ust. 7 RODO, jak i art. 46 ust. 2 lit. c) RODO, wówczas strony muszą polegać na standardowych klauzulach umownych w sprawie przekazywania danych.

4.2 Główne uwagi dotyczące załącznika do decyzji wykonawczej Komisji

4.2.1 Cel i zakres (klauzula 1 w projekcie standardowych klauzul umownych)

30. W **klauzuli 1.a** w projekcie standardowych klauzul umownych określono, że celem standardowych klauzul umownych jest zapewnienie zgodności z RODO i rozporządzeniem (UE) 2018/1725. EROD i EIOD są zdania, że strony umowy przy podpisywaniu klauzul powinny mieć możliwość wyboru odniesień do RODO lub rozporządzenia (UE) 2018/1725 w zależności od tego, które z tych rozporządzeń ma zastosowanie do ich sytuacji.

31. W ten sposób podmioty stosujące standardowe klauzule umowne na mocy art. 28 RODO nie miałyby w swoich standardowych klauzulach umownych odniesienia do rozporządzenia (UE) 2018/1725, a podmioty opierające się na art. 29 rozporządzenia (UE) 2018/1725 uniknęłyby odniesień do RODO. Przyczyniłoby się to do zwiększenia przejrzystości w stosunkach między stronami, które często są mniej zaznajomione z takimi przepisami. W takim przypadku w standardowych klauzulach umownych należy określić, że taki wybór jest możliwy, i odpowiednio dostosować brzmienie standardowych klauzul umownych.

32. Jak przewidziano w **klauzulach 1.b i 1.c**, a także zgodnie z **klauzulą 5** (klauzulą pozwalającą innym podmiotom na przystąpienie do umowy, zwaną dalej „klauzulą przystąpienia"), stronami standardowych klauzul umownych w odniesieniu do przetwarzania określonego w **załączniku II** może być kilku administratorów i kilka podmiotów przetwarzających, wymienionych w **załączniku I**. EROD i EIOD uważają, że w przypadku wielu stron umowy, standardowe klauzule umowne (i załączniki do nich) powinny nakładać na strony wymóg bardziej szczegółowego i precyzyjnego podziału obowiązków oraz wyraźnego wskazania, jaki rodzaj przetwarzania jest prowadzony przez który podmiot przetwarzający, w imieniu którego administratora i do jakich celów. Obecne sformułowanie tych klauzul w standardowych klauzulach umownych i załącznikach może prowadzić do nieporozumień co do kwalifikacji i roli każdego podmiotu w odniesieniu do danej operacji przetwarzania, zwłaszcza biorąc pod uwagę możliwość włączenia klauzuli przystąpienia.

4.2.2 Niezmienność (klauzula 2 w projekcie standardowych klauzul umownych)

33. Zgodnie z **klauzulą 2.b** w projekcie standardowych klauzul umownych strony zobowiązują się do niezmieniania dodatkowych klauzul, pod warunkiem że „nie są one bezpośrednio lub pośrednio sprzeczne" ze standardowymi klauzulami umownymi. Aby zapewnić administratorom i podmiotom przetwarzającym pewność prawa, EROD i EIOD z zadowoleniem przyjęliby wyjaśnienia dotyczące rodzaju klauzul, które Komisja Europejska uznałaby za bezpośrednio lub pośrednio sprzeczne ze standardowymi klauzulami umownymi. Wyjaśnienie takie mogłoby na przykład wskazywać, że klauzule sprzeczne ze standardowymi klauzulami umownymi to takie, które podważają lub negatywnie wpływają na obowiązki określone w standardowych klauzulach umownych lub uniemożliwiają przestrzeganie obowiązków określonych w standardowych klauzulach umownych. Na przykład klauzule zezwalające podmiotom przetwarzającym na wykorzystywanie danych do własnych celów byłyby sprzeczne z obowiązkiem podmiotu przetwarzającego do przetwarzania danych osobowych wyłącznie w imieniu administratora oraz do celów i przy użyciu środków określonych przez tego ostatniego.

4.2.3 Klauzula przystąpienia (klauzula 5 w projekcie standardowych klauzul umownych)

34. W **klauzuli 5** w projekcie standardowych klauzul umownych umożliwia się opcjonalnie każdemu podmiotowi przystąpienie do standardowych klauzul umownych, a tym samym zostanie nową stroną umowy jako administrator lub podmiot przetwarzający. Jak już wspomniano powyżej, kwalifikację i rolę takiej nowej strony umowy należy wyraźnie określić w załącznikach poprzez wezwanie stron do bardziej szczegółowego i precyzyjnego podziału obowiązków oraz wyraźnego wskazania, jaki rodzaj przetwarzania jest prowadzony przez który podmiot przetwarzający, w imieniu którego administratora i do jakich celów.

35. Zgodnie z **klauzulą 5.a** przystąpienie nowych stron do standardowych klauzul umownych jest uzależnione od zgody wszystkich pozostałych stron. W celu uniknięcia trudności w praktyce EROD i EIOD z zadowoleniem przyjęliby objaśnienie sposobu wyrażania takiej zgody przez pozostałe strony (czy powinna ona mieć formę pisemną, czy też nie, termin wyrażenia takiej zgody, informacje potrzebne przed wyrażeniem zgody). EROD i EIOD z zadowoleniem przyjęliby również wyjaśnienie, czy i w jaki sposób zgodę taką muszą wyrazić wszystkie strony, niezależnie od ich kwalifikacji i roli w przetwarzaniu.

4.2.4 Obowiązki stron (klauzula 7 w projekcie standardowych klauzul umownych)

36. Chociaż tytuł tej klauzuli brzmi „Obowiązki stron", **klauzula 7.a** w swojej obecnej formie odnosi się jedynie do obowiązków nałożonych na podmiot przetwarzający. Art. 28 ust. 3 RODO stanowi, że w umowie między administratorem a podmiotem przetwarzającym określono prawa, ale także obowiązki administratora. W związku z tym EROD i EIOD sugerują dodanie do tej klauzuli odniesienia do obowiązków nałożonych na administratora w celu zapewnienia kompletności i większej jasności. Na przykład przed klauzulą 7.a można by dodać następujące zdanie: „Administrator ma prawo i obowiązek podejmowania decyzji dotyczących celów i środków przetwarzania danych osobowych oraz jest odpowiedzialny za zapewnienie, aby przetwarzanie danych osobowych odbywało się zgodnie z mającymi zastosowanie przepisami UE lub państwa członkowskiego dotyczącymi ochrony danych oraz klauzulami (w tym za zapewnienie, aby przetwarzanie danych osobowych, do którego jest zobowiązany podmiot przetwarzający, opierało się na podstawie prawnej zgodnie z art. 6 RODO lub art. 5 rozporządzenia (UE) 2018/1725)".

37. Klauzula 7.a stanowi również, że polecenia powinny być wyszczególnione w załączniku IV oraz że późniejsze polecenia mogą być również wydawane przez administratora. Możliwość wydawania przez administratora „późniejszych poleceń" jest konieczna do pełnego wdrożenia praw i obowiązków stron określonych w standardowych klauzulach umownych, ale nie jest nieograniczona. Wszelkie późniejsze polecenia powinny być zgodne z odpowiednimi prawami i obowiązkami stron określonymi w standardowych klauzulach umownych. Zdaniem EROD i EIOD należy to jasno sprecyzować w klauzuli.

38. Dodatkowo w celu zwiększenia spójności z tekstem art. 28 ust. 3 lit. a) RODO i art. 29 ust. 3 lit. a) rozporządzenia (UE) 2018/1725 oraz w celu włączenia takiego obowiązku bezpośrednio do umowy EROD i EIOD proponują zmianę końca pierwszego zdania klauzuli 7.a poprzez nadanie mu następującego, podkreślonego brzmienia: „Podmiot przetwarzający przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora, chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający; w takim

przypadku przed rozpoczęciem przetwarzania podmiot przetwarzający informuje administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny".

39. Jeżeli chodzi o przypadek niezgodnych z prawem poleceń wydanych przez administratora, opisany w art. 28 ust. 3 akapit drugi RODO, EROD i EIOD są zdania, że umowa między administratorem a podmiotem przetwarzającym powinna zawierać bardziej precyzyjne informacje na temat konsekwencji i rozwiązań przewidzianych w przypadku, gdy podmiot przetwarzający poinformuje administratora, że jego zdaniem polecenie narusza przepisy RODO lub inne mające zastosowanie przepisy dotyczące ochrony danych. Dlatego też Komisja Europejska powinna zachęcić strony do zawarcia w umowie dalszych szczegółowych informacji dotyczących konsekwencji zgłoszenia poleceń naruszających prawo (np. klauzula o możliwości zawieszenia przez podmiot przetwarzający wykonania polecenia do czasu potwierdzenia, zmiany lub wycofania polecenia przez administratora, klauzula o rozwiązaniu umowy w przypadku nalegania przez administratora na wykonanie niezgodnego z prawem polecenia).

40. Jeżeli chodzi o opcje dostępne administratorowi zgodnie z **klauzulą 7.2**, odnoszące się do usuwania lub zwrotu danych, EROD i EIOD wzywają Komisję Europejską do określenia w samej klauzuli, że administrator powinien mieć możliwość zmiany wyboru dokonanego w momencie podpisania umowy przez cały okres obowiązywania umowy oraz po jej rozwiązaniu.

41. Tytułem uwagi ogólnej do **klauzuli 7.3** dotyczącej bezpieczeństwa przetwarzania EROD i EIOD zauważają, że wszystkie obowiązki spoczywają na podmiocie przetwarzającym, przy czym nie określono roli administratora, w szczególności jeżeli chodzi o ocenę ryzyka, którą należy przeprowadzić w odniesieniu do środków bezpieczeństwa z uwzględnieniem określonego przez administratora celu przetwarzania. W niektórych przypadkach podmiot przetwarzający może nie być świadomy dokładnego celu przetwarzania, na przykład kiedy przechowuje dane. Dlatego też, zgodnie z przepisami art. 28 ust. 3 RODO, EROD i EIOD są zdania, że klauzulę tę należy uzupełnić o obowiązki dotyczące bezpieczeństwa przetwarzania spoczywające na administratorze, który musi w szczególności dostarczyć podmiotowi przetwarzającemu wszystkie użyteczne informacje, aby ten mógł spełnić odpowiednie wymogi w tym zakresie.

42. W **klauzuli 7.3.a** w projekcie standardowych klauzul umownych przewidziano, że podmiot przetwarzający ma maksymalnie 48 godzin na zgłoszenie administratorowi naruszenia ochrony danych osobowych. W niektórych sytuacjach termin ten może być krótki i może być również mylony z terminem, w którym administrator musi zgłosić naruszenie ochrony danych osobowych organowi nadzorczemu (bieg tego terminu rozpoczyna się w chwili stwierdzenia naruszenia przez administratora, tj. w chwili otrzymania zgłoszenia od podmiotu przetwarzającego). Mając na uwadze spoczywający na podmiocie przetwarzającym wymóg zgłoszenia administratorowi naruszenia ochrony danych osobowych „bez zbędnej zwłoki" po jego stwierdzeniu, zgodnie z art. 33 ust. 2 RODO, EROD i EIOD sugerują jednak, aby – w zależności od sytuacji – pozostawić stronom możliwość określenia odpowiedniego terminu na dopełnienie tego wymogu. Należy zatem wymagać od stron, aby w standardowych klauzulach umownych określiły uzgodniony termin na dokonanie takiego zgłoszenia.

43. W **klauzuli 7.4.c** w projekcie standardowych klauzul umownych przewidziano możliwość skorzystania przez administratora, w celu przeprowadzania audytów, z usług niezależnego audytora wyznaczonego przez podmiot przetwarzający. Przepis ten nie jest przewidziany w art. 28 ust. 3 lit. h) RODO i należy go dostosować do tego artykułu, który stanowi, że podmiot przetwarzający musi umożliwić administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczynić się do nich. W związku z tym podmiot przetwarzający może

zaproponować audytora, ale decyzję o jego wyborze należy pozostawić administratorowi zgodnie z art. 28 ust. 3 lit. h) RODO.

44. **Klauzula 7.4.c** stanowi również, że jeżeli administrator zleca przeprowadzenie audytu niezależnemu audytorowi, ponosi koszty jego wynagrodzenia, a jeżeli podmiot przetwarzający zleca przeprowadzenie audytu – musi on ponieść koszty wynagrodzenia niezależnego audytora. Ponieważ kwestia podziału kosztów między administratora a podmiot przetwarzający nie jest uregulowana w RODO, EROD i EIOD uważają w związku z tym, że z klauzuli tej należy usunąć wszelkie odniesienia do kosztów.

45. W odniesieniu do **klauzuli 7.7** dotyczącej międzynarodowego przekazywania danych, w szczególności sytuacji, w której podmiot przetwarzający polega na podprzetwarzającym w państwie trzecim, EROD i EIOD wyrażają opinię, że w treści klauzuli 7.7.b można by bardziej sprecyzować możliwość podpisania przez te dwie strony jednego zbioru standardowych klauzul umownych w celu zapewnienia zgodności zarówno z rozdziałem V, jak i z art. 28 ust. 4 RODO, jeżeli taki jest rzeczywiście cel tej klauzuli, co wymagałoby dalszego wyjaśnienia. Należy również wyjaśnić, czy strony muszą opierać się na tym zbiorze klauzul, czy raczej na standardowych klauzulach umownych w sprawie przekazywania danych, które również zapewniają zabezpieczenia na podstawie art. 28 ust. 3 i 4 RODO.

46. Dodatkowo EROD i EIOD pragną podkreślić, że chociaż **klauzula 7.7.b** odnosi się tylko do stosowania standardowych klauzul umownych w sprawie przekazywania danych, można zgodnie z prawem opierać się na kilku innych narzędziach służących do przekazywania danych między podmiotem przetwarzającym a podprzetwarzającym w państwie trzecim, i w związku z tym sugerują użycie bardziej ogólnego sformułowania odnoszącego się do narzędzi przekazywania danych na podstawie art. 46 RODO.

47. EROD i EIOD stwierdziły również potrzebę dokładniejszego wyjaśnienia ostatniej części klauzuli 7.7.b, w której jest mowa o „warunkach stosowania" standardowych klauzul umownych w sprawie przekazywania danych. Ponieważ w przepisie tym sugeruje się, że mogą istnieć szczególne warunki stosowania standardowych klauzul umownych w sprawie przekazywania danych, należy określić, jakie są to warunki.

4.2.5 Prawa osoby, której dane dotyczą (klauzula 8 w projekcie standardowych klauzul umownych)

48. Obecnie klauzula ta nosi nazwę „Prawa osoby, której dane dotyczą", ale EROD i EIOD są zdania, że nazwa ta nie odzwierciedla treści klauzuli.

49. W istocie **klauzule 8.a i 8.b** w projekcie standardowych klauzul umownych odnoszą się do spoczywającego na podmiocie przetwarzającym obowiązku udzielenia administratorowi pomocy w wywiązaniu się z jego obowiązku udzielenia odpowiedzi na wnioski o wykonanie praw osoby, której dane dotyczą, określonych w rozdziale III RODO i w rozdziale III rozporządzenia (UE) 2018/1725. Klauzule 8.c i 8.d odnoszą się jednak do udzielania przez podmiot przetwarzający pomocy przy innych rodzajach obowiązków administratora, w szczególności na podstawie art. 32–36 RODO i art. 33–41 rozporządzenia (UE) 2018/1725.

50. EROD i EIOD sugerują zatem zmianę nazwy tej klauzuli na „Pomoc dla administratora", aby odzwierciedlić różne rodzaje pomocy, której musi udzielić podmiot przetwarzający.

51. Jako alternatywę EROD i EIOD zaleciłyby Komisji podzielenie tej klauzuli na dwie części, tak aby wprowadzić rozróżnienie na pomoc, której podmiot przetwarzający musi udzielić administratorowi:

- w wywiązaniu się z jego obowiązków dotyczących udzielenia odpowiedzi na wnioski o wykonanie praw osoby, której dane dotyczą, określonych w rozdziale III RODO i w rozdziale III rozporządzenia (UE) 2018/1725 oraz
- w wywiązaniu się z jego obowiązków na podstawie art. 32–36 RODO i art. 33–41 rozporządzenia (UE) 2018/1725.

52. Również w klauzuli 8.a w projekcie standardowych klauzul umownych przewidziano, że „podmiot przetwarzający niezwłocznie zawiadamia administratora danych o każdym wniosku, który wpłynął bezpośrednio od osoby, której dane dotyczą. Podmiot przetwarzający nie odpowiada na taki wniosek samodzielnie, jeżeli nie został do tego upoważniony przez administratora danych i do czasu uzyskania takiego upoważnienia".

53. Zdaniem EIOD i EROD w klauzuli tej należy:

- doprecyzować, że odpowiedzi osobom, których dane dotyczą, udziela się zgodnie z instrukcjami administratora (np. dotyczącymi treści odpowiedzi), jak określono w załączniku IV;
- doprecyzować, że zakres spoczywającego na podmiocie przetwarzającym obowiązku dotyczącego wykonywania praw osoby, której dane dotyczą, w imieniu administratora musi być opisany i wyraźnie określony w załączniku VII.

54. **Klauzula 8.c.1** i **klauzula 9.a** zawierają wymóg określenia właściwego organu nadzorczego, ale nie przewidziano w nich przypadku, w którym stronami umowy jest kilku administratorów, a tym samym kilka właściwych organów nadzorczych. Dlatego należy dodać możliwość podania kilku właściwych organów nadzorczych. Ponadto mogą wystąpić przypadki, w których przetwarzanie objęte zakresem klauzul ma charakter transgraniczny, a jako właściwy organ nadzorczy należy wskazać wiodący organ nadzorczy. Powinno to znaleźć odzwierciedlenie również w klauzuli 8.c.1 i w klauzuli 9.a.

55. EROD i EIOD sugerują, że w przypadku, gdy podmioty przetwarzające na terytorium UE podlegają przepisom lub praktykom państwa trzeciego, które mają wpływ na zgodność z tymi klauzulami, Komisja powinna ocenić, czy właściwa jest dodatkowa klauzula uwzględniająca takie przypadki.

4.2.6 Załączniki do projektu standardowych klauzul umownych

56. Standardowe klauzule umowne są przeznaczone do stosowania w umowach o przetwarzaniu danych, które mogą obejmować więcej niż jedną stronę jako administratora lub więcej niż jedną stronę jako podmiot przetwarzający. Wiąże się to z ryzykiem zatarcia odpowiedzialności stron w przypadku niewłaściwego wypełnienia załączników. Ryzyko to wzrasta, gdy do umowy przystępują później nowe strony poprzez zastosowanie klauzuli przystąpienia lub gdy umowa obejmuje przetwarzanie do różnych celów lub w różnych okolicznościach.

57. EIOD i EROD uważają, że niezwykle istotne jest, aby w załącznikach do standardowych klauzul umownych określono w sposób całkowicie przejrzysty role i obowiązki każdej ze stron w każdej relacji i w odniesieniu do każdej czynności przetwarzania. Jest to konieczne, aby strony mogły ustalić, kto przetwarza które dane osobowe, dla kogo i w jakim celu oraz jakie instrukcje mają zastosowanie i kto jest uprawniony do ich wydawania. Wszelkie niejasności uniemożliwiłyby administratorom lub podmiotom przetwarzającym wywiązanie się ze swoich obowiązków wynikających z zasady rozliczalności.

58. Jeżeli strony świadczące określone usługi przetwarzania lub korzystające z takich usług, opis (szczegóły) przetwarzania, mające zastosowanie środki techniczne i organizacyjne, instrukcje

administratora dotyczące przetwarzania danych osobowych, szczególne ograniczenia lub dodatkowe zabezpieczenia dotyczące danych należących do szczególnej kategorii, upoważnieni podprzetwarzający lub środki techniczne i organizacyjne, za pomocą których podmiot przetwarzający ma obowiązek udzielać pomocy administratorowi, różnią się między sobą, wówczas strony powinny mieć obowiązek wypełnienia kolejnych załączników I–VII, chyba że różnice te są bardzo niewielkie, a wyjątki zostały wyraźnie opisane w załącznikach.

59. W przypadku złożonej umowy, która na przykład obejmuje kilka stron lub ma kilka celów, zawsze musi jednoznacznie wynikać, który załącznik (lub w przypadku ograniczonych odstępstw w ramach jednego załącznika: które postanowienie w tym załączniku) ma zastosowanie do której konkretnej sytuacji lub relacji. Należy wyraźnie określić i rozróżnić poszczególne czynności przetwarzania.

***

W imieniu Europejskiego Inspektora Ochrony Danych

Europejski Inspektor Ochrony Danych

(Wojciech Wiewiórowski)

W imieniu Europejskiej Rady Ochrony Danych

Przewodnicząca

(Andrea Jelinek)



Opinion 18/2021 on the draft Standard Contractual Clauses submitted by the LT SA (Article 28(8) GDPR)

Adopted on 19 May 2021

TABLE OF CONTENTS

1 Summary of the Facts 4
2 Assessment 4
2.1 General reasoning of the Board regarding the set of standard contractual clauses 4
2.2 Analysis of the draft decision and of the draft standard contractual clauses 5
2.2.1 General remark on the whole SCCs and on the draft decision 5
2.2.2 Purpose of the agreement (Chapter I of the SCCs) 6
2.2.3 Obligation of the parties (Chapter II of the SCCs) 6
2.2.4 Confidentiality (Chapter III of the SCCs) 7
2.2.5 Security of processing (Chapter IV of the SCCs) 7
2.2.6 Engagement of other data processor (Chapter V of the SCCs) 8
2.2.7 Transfer of data to third countries or international organisations (Chapter VI of the SCCs) 9
2.2.8 Assistance to the data controller (Chapter VII of the SCCs) 9
2.2.9 Notification of personal data breach (Chapter VIII of the SCCs) 10
2.2.10 Erasure and return of data (Chapter IX of the SCCs) 11
2.2.11 Control of the data processor / Audit and inspection (Chapter X of the SCCs) 11
2.2.12 Final provisions (Chapter XI of the SCCs) 11
2.2.13 Annex 1 11
2.2.14 Annex 2 12
2.2.15 Annex 3 12
3 Conclusions 13
4 Final Remarks 13

The European Data Protection Board

Having regard to Article 28(8), Article 63 and Article 64(1)(d), (3) - (8) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter, "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,[1]

Having regard to Article 10 and 22 of its Rules of Procedure of 25 May 2018,

Whereas:

(1) The main role of the European Data Protection Board (hereinafter, the "Board") is to ensure the consistent application of the GDPR throughout the Union. To this end, the Board shall issue an opinion based on Article 64(1)(d) GDPR where a supervisory authority (hereinafter, "SA") aims to determine standard contractual clauses (hereinafter, also "SCCs") referred to in Article 28(8) GDPR. The aim of this Opinion is therefore to contribute to a harmonised approach concerning measures to be adopted by a supervisory authority that are intended to produce legal effects as regards processing operations which substantially affect a significant number of data subjects in several Member States and the consistent implementation of the GDPR's specific provisions.

(2) In the context of the relationship between a data controller and a data processor (or data processors) for the processing of personal data, the GDPR establishes, in its Article 28, a set of provisions with respect to the setting up of a specific contract between the parties involved and to mandatory provisions that should be incorporated in it.

(3) According to Article 28(3) GDPR, the processing by a data processor "*shall be governed by a contract or other legal act under Union or Member State law that is binding on the processor with regard to the controller*"; a set of specific aspects to regulate the contractual relationship between the parties is therefore set out, including among others, the subject-matter and duration of the processing, its nature and purpose, the type of personal data and categories of data subjects.

(4) Under Article 28(6) GDPR, without prejudice to an individual contract between the data controller and the data processor, the contract or the other legal act referred in paragraphs (3) and (4) of Article 28 GDPR may be based, in whole or in part, on standard contractual clauses. These standard contractual clauses are to be adopted for the matters referred to in paragraphs (3) and (4).

(5) Furthermore, Article 28(8) GDPR determines that a SA may adopt a set of standard contractual clauses in accordance with the consistency mechanism referred to in Article 63. In this regard, SAs are required to cooperate with other members of the Board and, where relevant, with the European Commission through the consistency mechanism. Pursuant to Article 64(1)(d), SAs are required to communicate to the Board any draft decision aiming to determine standard contractual clauses pursuant to Article 28(8). In this context, the Board is required to issue an opinion on the matter, pursuant to Article 64(3), where it has not already issued an opinion on the same matter.

(6) Adopted standard contractual clauses constitute a set of guarantees to be used as is, as they are intended to protect data subjects and mitigate specific risks associated with the fundamental principles of data protection.

(7) The opinion of the Board shall be adopted pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete (unless the period is extended upon decision of the Chair by a further six weeks).

HAS ADOPTED THE OPINION:

1 SUMMARY OF THE FACTS

1. The Lithuanian supervisory authority (hereinafter, "LT SA") has submitted its draft decision and its draft standard contractual clauses to the Board, requesting its opinion pursuant to Article 64(1)(d), for a consistent approach at Union level. After the decision on the completeness of the file, the EDPB Secretariat circulated the file to all members on behalf of the Chair on 26 March 2021.
2. The Board has received the draft SCCs from the LT SA along with a draft decision explaining the background and role of the standard contractual clauses. These two documents were provided by the LT SA in an English version.

2 ASSESSMENT

2.1 General reasoning of the Board regarding the set of standard contractual clauses

3. Any set of standard contractual clauses submitted to the Board under Article 28(8) and Article 64(1)(d) must further specify the provisions foreseen in Article 28 GDPR. The opinion of the Board aims at ensuring consistency and a correct application of Article 28 GDPR as regards the presented draft clauses, which could serve as Art. 28(8) standard contractual clauses.
4. The Board notes that the draft SCCs presented to the Board are composed of two parts:
    1) a general part containing general provisions to be used "as is"; and
    2) a specific part that has to be completed by the parties with regard to the specific processing which the contract seeks to govern.
5. The Board recalls that the evaluation of each draft decision subject to the consistency mechanism is made individually and on its own merits, bearing in mind the goal of ensuring consistency.

[1] References to the "Union" or the "EU" made throughout this Opinion should be understood as references to the "EEA".

6. The EDPB has already expressed its views on draft standard contractual clauses for the purposes of compliance with Article 28 GDPR in EDPB Opinion 14/2019[2], EDPB Opinion 17/2020[3], and EDPB-EDPS Joint Opinion 1/2021[4].

7. When this opinion remains silent on one or more clauses of the SCCs submitted by the LT SA, it means that the Board is not asking the LT SA to take further action with regard to those specific clauses.

2.2 Analysis of the draft decision and of the draft standard contractual clauses

2.2.1 General remark on the whole SCCs and on the draft decision

8. Since a contract under Article 28 GDPR should further stipulate and clarify how the obligations in Article 28(3)-(4) will be fulfilled, the SCCs need to be analysed in their entirety.

9. In addition, the Board recalls that the possibility to use Standard Contractual Clauses adopted by a supervisory authority does not prevent the parties from adding other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, the adopted standard contractual clauses or prejudice the fundamental rights or freedoms of the data subjects. Furthermore, where the standard data protection clauses are modified, the parties will no longer be deemed to have implemented adopted standard contractual clauses. Consequently, the Board recommends that the LT SA replace the words "*if they directly or indirectly contradict*" in the draft decision (paragraph 2) by "*as long as they do not directly or indirectly contradict*".

10. The Board notes that the wording of several clauses of the SCCs in the English version provided are not in line with the terminology of the relevant provisions of the GDPR. Examples include: "*controller's duties*" (used instead of "*controller's obligations*"), "*Union or Member State legal acts*" (used instead of "*Union or Member State law*"), "*permission*" (used instead of "*authorization*"), "*prove*" (used instead of "*demonstrate*"), "*special*" (used instead of "*specific*"). The Board therefore recommends the LT SA to align the wording of those clauses with the relevant provisions of the GDPR.

11. Further, the Board is of the opinion that the use of the word "Agreement" to designate SCCs may trigger confusion between this contractual document which serve as Article 28(8) GDPR standard contractual clauses and other possible agreements that might be concluded by the Parties. For the sake of clarity, the Board recommends that the LT SA replace the words "Agreement" by "Standard Contractual Clauses" or "Clauses" where referring to the aforementioned SCCs, in the whole draft decision and in the whole annex.

12. The Board recommends removing the reference to "*other mutual agreements*" from page 1 (last paragraph) of the draft SCCs as it seems to imply that additional clauses or agreements entered into by the parties fall within the scope of the SCCs themselves.

13. Finally, the Board is of the opinion that a specific provision on the definition of the terms used in the Clauses might be added to the SCCs in order to avoid any difficulties in practice. The Board therefore encourages the LT SA to specify that whenever the Clauses use the terms defined in the GDPR, those terms have the meaning given to such terms by the GDPR itself.

2.2.2 Purpose of the agreement (Chapter I of the SCCs)

14. Regarding **clause 2** of the SCCs, the Board is of the opinion that the wording "*[where applicable, details of the agreement on provision of such services]*" is not fully clear, and encourages the LT SA to further clarify which type of details the parties would be expected to insert. As an example, the clause may be redrafted as follows: "*[where applicable, specify details on the agreement entered into by the Parties on these services, e.g. date / title]*". In addition, and in order to avoid any doubt regarding what should be filled in by the Parties in Annex 1, the Board encourages the LT SA to replace the words "*including but not limited to the subject, purpose and nature of the processing of personal data, types of personal data, categories of the data subjects etc.*" with a direct reference to Annex 1.

2.2.3 Obligation of the parties (Chapter II of the SCCs)

15. Regarding **clause 3** of the SCCs, the Board is of the opinion that the reference to commitments that the controller "shall undertake" may be misleading in the context of a contract because the rights and obligations of the controller described in clause 3 are already vested in the controller by the GDPR, and that it should be deleted. In addition, this clause would be clearer if a reference to Article 24 GDPR and its accountability principle were made. Consequently, the Board recommends that clause 3.1 be modified, for instance, as follows: "*[The Data Controller] is responsible for ensuring that the processing of personal data takes place in compliance with Regulation (EU) 2016/679 (see Article 24 GDPR) […]*".

16. Regarding **clause 3.2** of the SCCs, since the controller has already defined the purposes and means of the processing activity subject to the SCCs, the Board recommends to the LT SA to rephrase it as follows: "*3.2 [The Data Controller] has the right and obligation to make decisions about the purposes and means of the processing of personal data*".

17. Regarding **clause 3.3** of the SCCs, the Board is of the opinion that it should be clarified that the obligation of the controller is not limited to the identification of the legal basis, and thus recommends that the clause be redrafted as follows: "*3.3 [The Data Controller] shall be responsible, among others, for ensuring that the processing of personal data which the data processor is instructed to perform has a legal basis.*"

18. Regarding **clause 4.1** of the SCCs, third sentence, the Board is of the opinion that the possibility for the controller to give subsequent or further instructions is necessary to fully implement the rights and obligations of the parties set out in the clause 4, but is not unlimited. Any subsequent instruction should be in line with the respective rights and obligations of the parties set out in the SCCs. For the sake of clarity, the EDPB therefore encourages the LT SA to specify this in the clause.

[2] EDPB Opinion 14/2019 on the draft Standard Contractual Clauses submitted by the DK SA (Article 28(8) GDPR), adopted on 9 July 2019, available here: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinion_201914_dk_scc_en.pdf ; The final version of the standard contractual clauses for the purposes of compliance with Article 28 GDPR adopted by the Danish SA is available here: https://edpb.europa.eu/our-work-tools/our-documents/decisionsa/dk-sa-standard-contractual-clauses-purposes-compliance-art_en.

[3] EDPB Opinion 17/2020 on the draft Standard Contractual Clauses submitted by the SI SA (Article 28(8) GDPR), adopted on 19 May 2020, available here: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinion_202017_art28sccs_si_en.pdf.

[4] EDPB-EDPS Joint Opinion 1/2021 on the draft Standard Contractual Clauses submitted by the European Commission (Article 28(7) GDPR), adopted on 19 May 2020, available here: https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-12021-standard_en.

19. Furthermore, the Board considers that where the processor processes the data not under the instructions of the controller but because it is required to do so by Union or Member State law to which it is subject, then the processor shall inform the controller of the legal requirement before the processing of this data, unless that law prohibits such information on important grounds of public interest. The Board therefore recommends to the LT SA to include this specification.

2.2.4 Confidentiality (Chapter III of the SCCs)

20. Regarding **clause 7** of the SCCs, first sentence, the Board recommends, for the sake of consistency and clarity, that the LT SA bring the wording in line with Article 28(3)(b) GDPR and refer explicitly to the principle of the access to the personal data on a "need-to-know" basis. The Board would therefore suggest the following wording: "*under the processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need to know basis*". Furthermore, the Board encourages the LT SA to split the following part of clause 7 into different paragraphs and introduce some amendments in order to enhance its clarity: clause 7 can therefore be reorganised as follows: "*7. […] The Parties ensure that: 7.1. In case of a need to change in the persons having access to personal data, their right of access to the Data Controller's personal data shall be revoked not later than on the last day on which their tasks require them to have access to the personal data of the Data Controller entrusted to the Processor. In case of discontinuation of employment relationship with the employee of the Data Processor, the access rights to the Data Controller's personal data shall be revoked not later than on the last day of work. 7.2 The list of persons granted access to personal data shall be reviewed on a periodical basis […]*".

2.2.5 Security of processing (Chapter IV of the SCCs)

21. Regarding **clause 9** of the SCCs, the Board recommends that the LT SA specify that the level of the risk should take into account "*the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons*", which corresponds to the wording of Article 32(1) GDPR. This specific wording is used in the GDPR to make sure that the level of security applied to the processing of personal data is always in line with the latest technological evolutions.

22. Regarding **clause 11** of the SCCs, the Board encourages the LT SA to delete "*which may arise*" and to replace "*minimise the risk*" by "*mitigate the risk*". In addition, the Board recommends to the LT SA to clarify that "*independently from the controller*" refers to the assessment of the risk, rather than to the implementation of measures, which in the current wording is not entirely clear. As an example, the first sentence of the clause may be redrafted as follows: "*According to Article 32 GDPR, the data processor shall also – independently from the data controller – evaluate the risks to the rights and freedoms of natural persons inherent in the processing activity entrusted to it by the controller, and implement measures to mitigate those risks*".

23. Regarding **clause 12** of the SCCs, the Board recommends that the LT SA align the wording with Article 28(3)(f) GDPR, by referring to assistance to the controller in ensuring compliance with the obligation (instead of "*fulfilment*" of its "*duties*") provided for in Article 32 GDPR.

24. Regarding **clause 13** of the SCCs, the Board understands that the first sentence refers to the case where subsequently, in the assessment of the controller, the mitigation of the identified risks requires further measures to be implemented by the processor. If it is the case, the Board recommends to the LT SA to clarify this. As regards the second sentence of the clause, the Board is of the opinion that it

may be misleading to specify the right of the controller to obtain evidence of implementation of such supplementary measures, considering that the audit right of the controller applies more broadly to all the obligations laid down in these SCCs as provided for in Article 28(3)(h) GDPR. The Board therefore recommends to the LT SA to amend this sentence and make reference to Chapter X of the SCCs (e.g. "*The Data Processor shall make available to the Data Controller all information necessary to demonstrate compliance with its obligations as provided in Chapter X of the Clauses*").

2.2.6 Engagement of other data processor (Chapter V of the SCCs)

25. Regarding Chapter V of the SCCs, the Board encourages the LT SA to slightly rephrase several sentences in order to clarify them. In clause 16, "*for the performance of this Agreement*" could be redrafted as "*for the performance of the processing carried out under this Agreement*". In clause 16.1, the words "*to the date of engagement*" can be replaced by "*before the date of engagement*". In clause 16.2, "*no later than till [specify the period]*" can be replaced by "*no later than [specify the period] in advance*" and "*special additional*" by "*specific*". Finally, the Board suggests avoiding repetition of the reference to Annex 2 in the latest sentences of clauses 16.1 and 16.2 which is already stated in clause 15.

26. Regarding **clause 17** of the SCCs more specifically, the reference to the possibility to enter into a contract or another legal act as currently included in the draft SCCs seems to be potentially misleading. Therefore, the Board recommends that this clause should be aligned with the wording of Article 28(4). In addition, the Board considers that it should specified in this clause that prior to the processing, the data processor shall inform the sub-processor of the identity and contact details of the controller for which the sub-processor processes personal data. The Board encourages the LT SA to rephrase the clause accordingly, for example as follows: "*Where the Processor engages a sub-processor for carrying out the particular processing on behalf of the Controller, the same data protection obligations as set out between the controller and the processor shall be imposed on the sub-processor by way of a contract or another legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organizational measures so that processing meets the requirements of Regulation (EU) 2016/679. Prior to processing, the data processor shall inform the sub-processor of the identity and contact details of the controller for which the sub-processor processes personal data*".

27. Regarding **clause 18** of the SCCs, the Board notes that the suggested obligation for the processor to provide a copy of the contract with the sub-processor where there is an impact on the instructions or the level of security is not explicitly provided by the GDPR and may be of unclear application for the parties, but understands the intention of requiring the processor to notify the controller in case of issues arising in connection with the engaged sub-processor. The Board recommends therefore that the LT SA replace this provision with the obligation for the processor to notify to the controller any failure by the sub-processor to fulfil its obligations under the contract or other legal act binding on this sub-processor. Finally, the last sentence should be rephrased as follows: "*The Data Processor is not obliged to provide the provisions of the Agreement on the business-related issues which do not have an impact on the terms and conditions of the legal protection of personal data of the contract concluded with the sub-processor*".

28. Regarding **clause 19** of the SCCs, the Board understands that the intention is to create a "third party beneficiary right" for the controller within the contract between the data processor and the sub-processor. Therefore, the Board encourages the LT SA to clarify the nature of the clause for instance by redrafting the first sentence as follows: the processor "*shall agree on a third-party beneficiary*

clause with a sub-processor (if any) providing that […]". The Board also recommends that "*continue data processing relationship directly with the sub-processor*" should be replaced with "*enforce the agreement directly against the sub-processor*". Additionally, the Board recalls that it sees an added value in having such a clause as part of a standard contractual clauses as it preserves the rights of the controller and therefore recommends to the LT SA to transform it into a non-optional clause.

29. Regarding **clause 20** of the SCCs, the Boards encourages the LT SA to include a reminder that the "*The data processor shall be responsible for requiring that the sub-processor at least complies with the obligations to which the data processor is subject pursuant to the Clauses and the GDPR*".

2.2.7 Transfer of data to third countries or international organisations (Chapter VI of the SCCs)

30. The Board encourages to the LT SA to clarify that the words "third countries" refer to countries outside of the EEA and not outside of Lithuania. This could be carried out by adding in **clause 21** "*[…] third countries (i.e. countries outside of the European Economic Area) […]*".

31. In addition, the Board recommends the deletion of footnote 2 in clause 21 and of the same sentence in Annex 3, Point 6 due to the fact that such standard contractual clauses do not appear as the relevant document to elaborate on the definition of the notion of transfers of personal data.

32. Regarding **clause 22** of the SCCs, the Board recommends to replace the wording "*transfer of such information*" with "*communication of such information*", in order to avoid any confusion with the notion of transfer as referred to in Chapter V of the GDPR.

33. Regarding **clause 23.1** of the SCCs, the Board encourages the LT SA to clarify the wording as follows: "*to transfer personal data to a Data Controller or a Data Processor in a third country or in an international organisation*".

34. The Board considers that mentioning the chosen tool for transfers, in addition to the instructions, contributes to demonstrating compliance of the parties with Chapter V of the GDPR; therefore, the EDPB encourages the LT SA to further clarify **clause 24** of the SCCs as follows: "*The data controller's instructions or approval regarding transfers of personal data to a third country including, if applicable, the transfer tool under Chapter V of Regulation (EU) 2016/679 on which they are based, shall be set out in Annex 3 of these standard contractual clauses*".

2.2.8 Assistance to the data controller (Chapter VII of the SCCs)

35. The Board encourages, for the sake of clarity as well as consistency with Article 28(3)(e) GDPR, the LT SA to slightly rephrase the **clause 26** of the SCCs as follows: "*Taking into account the nature of processing, the Data Processor shall assist the Data Controller to fulfil the Data Controller's obligation to respond to the requests for exercise of the data subject's rights provided for in Chapter III of Regulation (EU) 2016/679 by appropriate technical and organisational measures insofar as this is possible. This implies that the Data Processor shall, insofar as this is possible, assist the Data Controller in its obligation to give effect to the following data subject rights*".

36. Regarding **clause 27** of the SCCs, the Board notes that the content of this clause is repeated in **clause 29.** The Board therefore encourages the LT SA to merge clause 27 into clause 29, so that the new clause is aimed to ensure that the parties detail the arrangements on the manner the processor is bound to assist the controller relating to data subject rights and data breaches in Annex 3. By way of

example, the new clause could read as follows: "*The Parties shall establish in Annex 3 hereto the appropriate technical and organisational measures which should be taken by the Data Processor to assist the Data Controller with data subject rights and with the obligations under Articles 33 to 36 GDPR, as set out in paragraphs 26 and 27 hereof*".

37. The Board understands that **clause 28** of the SCCs, coupled with clause 12, is aimed to reflect the content of Article 28(3)(f) GDPR: while clause 12 refers to the processor's assistance with compliance with Article 32 GDPR, clause 28 covers the processor's assistance with compliance with Articles 33 to 36 GDPR. As a consequence, the Board recommends that clause 28 refer to clause 12 (rather than 13), and to redraft the clause to ensure closer consistency with the relevant provisions of the GDPR. The clause could be redrafted, for instance, as follows:

"*In addition to the Data Processor's duty to assist the Data Controller in accordance with paragraph 12 hereof, the Data Processor, taking into account the nature of processing and information available to the Data Processor, shall also assist the Data Controller in ensuring compliance with:*
28.1 the Data Controller's obligation to, without undue delay and where feasible, […];
28.2 *the Data Controller's obligation to notify without undue delay* […]
28.3 *the Data Controller's obligation to carry out a data protection impact assessment* […] *where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons.*
28.4 *the Data Controller's obligation to consult the competent supervisory authority […] if the data protection impact assessment indicates that processing of data would result in high risk if the Data Controller fails to take measures to mitigate the risk*".

2.2.9 Notification of personal data breach (Chapter VIII of the SCCs)

38. **Clause 30** of the SCCs, second sentence, recommends to the Parties to select a number of hours by which the processor shall notify a data breach which does not exceed 24 hours from the moment of becoming aware of the personal data breach. Such delay may be short in some situations and may also trigger confusion with the delay by which the controller has to notify the personal data breach to the SA. While taking into account the requirement for the processor to notify the controller "*without undue delay*" after becoming aware of the personal data breach in accordance with Article 33.2 GDPR, the Board recommends the LT SA to delete the sentence recommending that the timeframe (which anyways starts from the moment of becoming aware of the personal data breach - the word "breach" is missing) should not exceed 24 hours and allow the parties to choose the appropriate timeframe. Additionally, the Board recommends the deletion of "*If possible*" from the second sentence of clause 30 taking into account that a processor has in any event an obligation to proceed to such notification (Article 33.2 GDPR) and to avoid giving rise to situations where the processor may argue it was "impossible" to notify the controller concerning the data breach within the agreed timeframe.

39. Regarding **clause 31.4** of the SCCs, the Board encourages the LT SA to refer to the "*request of the competent supervisory authority*" instead of the "*letters of the competent supervisory authority*", since a supervisory authority might request information by means other than letters.

40. Regarding **clause 32** of the SCCs, pertaining to the obligation of the processor to notify additional information in case it fails to provide all information on the occasion of the first notification, the Board recommends that the LT SA remove the reference to 24 hours. Instead, it should be made clear that this information must be provided "*without undue further delay*" (instead of "*immediately*") in accordance with the controller's obligation under Article 33(4) GDPR.

2.2.10 Erasure and return of data (Chapter IX of the SCCs)

41. Regarding **clause 34** of the SCCs, the Board recommends that the LT SA specify that the options provided by this clause are left "*at the choice of the controller*" in order to more closely match the wording of Article 28(3)(g) GDPR. In addition, the Board suggests replacing "confirm" by "demonstrate". Thirdly, the Board recommends clarifying that the deletion of existing copies must be carried out "in any event" (the sentence could be thus rephrased as "*[…] and in any event delete the existing copies unless […]*"). Finally, the Board recommends that the LT SA detail in the clause itself that the controller should be able to modify the choice made at the time of signature of the contract throughout the life cycle of the contract and upon its termination.

2.2.11 Control of the data processor / Audit and inspection (Chapter X of the SCCs)

42. The Board understands that the Chapter X is referring to Article 28(3)(h) GDPR. The Board therefore encourages the LT SA, for purposes of clarification about the content of this Chapter, to rephrase the **title** of Chapter X as follows: "Audit and inspection of the data processor".

43. Regarding **clause 37** of the SCCs, the Board encourages the LT SA, for the sake of consistency with the GDPR, to slightly rephrase this clause to align it with the terminology of Article 28(3)(h) GDPR: "*The Data Processor shall make available the Data Controller with all information necessary to demonstrate compliance with the obligation set out in Article 28 of Regulation (EU) 2016/679 and the Agreement and enable and assist the Data Controller or another auditor mandated by the Data Controller to carry out an audit including on-the-spot inspections*".

44. Regarding **clause 39** of the SCCs, the Board is of the opinion that the wording "physical means" might be misleading. The Board therefore encourages the LT SA to rather refer to "physical facilities". Further, it may be advisable to specify within the SCCs that the controller and processor commit to cooperating with the Supervisory Authority, including by making available to the authority upon request information aimed to demonstrate compliance, including the results of audits and inspections.

2.2.12 Final provisions (Chapter XI of the SCCs)

45. Regarding **clause 44** of the SCCs, the Board encourages the LT SA to clarify the terms "*materially or regularly breaches the Agreement*" in order to avoid any confusion as to their interpretation by the Parties. In addition to the termination provisions of clause 44, the Board recommends that the SCCs include the possibility for the controller to terminate the SCCs where the clauses have been suspended in accordance with clause 43 of the SCCs and where compliance has not been restored within a certain amount of time to be determined by the Parties.

2.2.13 Annex 1

46. While noting that Annex 1 aims at providing details about the processing activities undertaken by the processor on behalf of the controller, the Board recalls that the processing activities should be described by the parties in the most detailed manner possible. Consequently, the Board welcomes the examples provided by the LT SA to illustrate the possible content of the sections of the Appendix as they are able to guide the parties' description.

47. The Board is nonetheless of the opinion that slight clarifications can be made on the level of detail expected in the Annex 1. The Board therefore encourages the LT SA to refer to "*processing activities*" instead of "*processing operations*" in point 1 of the Annex 1, as well was to "*types of personal data*" instead of "*personal data*" in point 1.3 of the Annex 1.

2.2.14 Annex 2

48. Regarding **point 1** of Annex 2, the Board welcomes the inclusion of a table guiding the Parties in the description of authorised sub-processors as provided for in Chapter V of the SCCs.

49. With regard to **point 2** of Annex 2 on prior notification for granting permission to new sub-processors, the Board encourages the LT SA to clarify that this point refers to new sub-processors, not already listed in the previous point. Also, the Board is of the opinion that the first sentence in its current form may be interpreted as contradicting clauses 16.1 and 16.2 which require that a specific period is set, and recommends that the LT SA rephrase the first sentence in order to guarantee that both the period of prior notification and the related terms and conditions are provided by the Parties: "*Please specify the periods of a prior notification of granting permission to the sub-processors and other related terms and conditions*".

2.2.15 Annex 3

50. Regarding Annex 3 of the SCCs, the Board is of the opinion that several sentences might be rephrased in order to avoid any confusion as to what it is expected to be filled in by the Parties. The Board therefore encourages the LT SA to refer to "'*the processing entrusted*" instead of "*the processing assigned*" (point 1), to "*elements*" instead of "*lots*" (point 2), to "*communication of the data*" instead of "*transfer of the data*"(point 2), to "*demonstrate the fact of erasure*" instead of "*prove the fact of erasure*" (point 4), to "*data processing location*" instead of "*data processing place*" (point 5) to "*information*" instead of "*familiarisation*" (points 7 and 8), and to "*physical facilities*" instead of "*physical measures*" (points 7 and 8).

51. As a general remark with respect to **point 2** of Annex 3, relating to Security of Processing, the Board recalls that the degree of detail of the information provided therein must be such as to enable the controller to assess the appropriateness of the measures, in order to comply with its obligation of accountability. Also, a suggestion for the parties to include a description of the measures for the protection of software applications used to process personal data could be useful.

52. Regarding **point 3** of Annex 3 related to the Assistance to Data Controller, the Board is of the opinion that the annex should include the steps to be taken by the processor and the procedure to be followed in providing assistance to the controller with regard to both Article 28(3)(e) and 28(3)(f) GDPR. For example, with regard to the obligation of assistance under Article 28(3)(e) GDPR, it has to be clear in the SCCs whether the data processor is expected to have any contact with the data subjects, and how the processor needs to inform the controller when it comes to data subjects' rights (e.g. forwarding the request to the controller within a specified timeframe or other appropriate measures). In this case, the assistance is provided only through an exchange of information between the controller and the processor. Another scenario could be that the controller instructs the processor to answer to data subject's requests according to instructions given. Another option could be that the processor would make the technical implementations instructed by the controller with respect to data subject rights. The Board suggests that the LT SA gives examples of organisational measures under which the cooperation of the processor might be provided in order to indicate the level of detail expected to be filled in by the Parties in Annex 3.

53. The Board also notes that **points 7 and 8** of the Annex 3 state that where the controller carry out a physical examination/on-spot inspection of the processor and sub-processor, it shall bear the costs. As to the issue of allocation of costs between a controller and a processor is not regulated by the GDPR, the Board consequently encourages the LT SA to remove any reference to the costs from these clauses.

3 CONCLUSIONS

54. The Board very much welcomes the Lithuanian SA's initiative to submit its draft SCCs for an opinion which aims at contributing to a harmonised implementation of the GDPR.

55. The Board is of the opinion that the draft SCCs of the Lithuanian Supervisory Authority submitted for an opinion need some further adjustments in order to be considered as standard contractual clauses. If all recommendations listed in this Opinion are implemented, the LT SA will be able to use this draft agreement as Standard Contractual Clauses pursuant to Article 28(8) GDPR without any need for a subsequent adoption from the EU Commission.

4 FINAL REMARKS

56. This opinion is addressed to the Lithuanian *Valstybinė duomenų apsaugos inspekcija* (the Lithuanian Supervisory Authority) and will be made public pursuant to Article 64 (5)(b) GDPR.

57. According to Article 64 (7) and (8) GDPR, the supervisory authority shall communicate to the Chair by electronic means, within two weeks after receiving the opinion, whether it will amend or maintain its draft SCCs. Within the same period, it shall provide the amended draft SCCs or, alternatively, the relevant grounds for which it does not intend to follow this opinion, in whole or in part. The supervisory authority shall communicate the final decision to the Board for inclusion in the register of decisions which have been subject to the consistency mechanism, in accordance with Article 70(1)(y) GDPR.

For the European Data Protection Board

The Chair

(Andrea Jelinek)



Opinion 17/2021 on the draft decision of the French Supervisory Authority regarding the European code of conduct submitted by the Cloud Infrastructure Service Providers (CISPE)

Adopted on 19 May 2021

Table of contents

1 SUMMARY OF THE FACTS....4
2 ASSESSMENT....4
2.1 The Code of conduct meets the needs of the sector....4
2.1.1 Presentation of the sector....4
2.1.2 The code owner as a representative organisation....5
2.1.3 Processing Scope....5
2.1.4 Territorial scope....6
2.2 The code of conduct facilitates the effective application of the GDPR....6
2.2.1 The code as a practical tool....6
2.2.2 Matrix of requirements....6
2.2.3 Binding nature of the Code....6
2.2.4 The Code provides sufficient safeguards....6
2.2.5 The Code as an accountability tool....7
2.3 The code of conduct provides effective mechanisms for monitoring compliance with a code 7
2.3.1 Adherence to the Code....7
2.3.2 The monitoring of the Code....7
2.3.3 Sanctions....8
2.3.4 The review of the code....8
3 CONCLUSIONS / RECOMMENDATIONS....8
4 FINAL REMARKS....8

The European Data Protection Board

Having regard to Article 63, Article 64(1)(b) and Article 40 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter "GDPR"),

Having regard to the European Economic Area (hereinafter "EEA") Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018[1],

Having regard to Articles 10 and 22 of its Rules of Procedure.

Whereas:

(1) Member States, Supervisory Authorities, the European Data Protection Board and the European Commission shall encourage the drawing up of codes of conduct (hereinafter "code") to contribute to the proper application of the GDPR[2].

(2) The main role of the European Data Protection Board (hereinafter "the EDPB") is to ensure the consistent application of the GDPR when a supervisory authority (hereinafter "SA") intends to approve a code of conduct that related to processing activities in several Member States (hereinafter "transnational code") pursuant to article 40.7 GDPR and to the Board's "Guidelines 1/2019 on Codes of Conduct and Monitoring bodies under Regulation 2016/679" (hereinafter the "Guidelines").

(3) The EDPB welcomes and acknowledges the efforts made by the associations and others bodies representing categories of controllers or processors to elaborate codes of conduct which are practical and potentially cost-effective tools to ensure greater consistency among a sector and foster the right to privacy and data protection of data subjects by increasing transparency.

(4) This opinion aims to ensure the consistent application of the GDPR, including by the SAs, controllers and processors and to highlight the core elements which each code of conduct has to develop.

(5) Taking into account the specific characteristics of the sector concerned, each code of conduct should be addressed individually and is without prejudice of the assessment of any other code of conduct. The EDPB recalls that Codes represent an opportunity to establish a set of rules which contribute to the proper application of the GDPR in a practical, transparent and potentially cost-effective manner that takes on board the specificities for a particular sector and/or its processing activities.

(6) The EDPB underlines that codes of conduct are voluntary accountability tools, and that the adherence to a code does not prevent DPAs from exercising their enforcement power and prerogatives.

[1] References to "Member States" made throughout this opinion should be understood as references to "EEA Member States".
[2] Article 40(1) of the GDPR

(7) The present code is not a code of conduct according to article 46(2)(e) meant for international transfers of personal data and therefore does not provide appropriate safeguards within the framework of transfers of personal data to third countries or international organisations under the terms referred to in point (e) of article 46 (2). Indeed, any transfer of personal data to a third country or to an international organisation shall take place only if the provisions of chapter V of the GDPR are respected.

(8) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in the guidelines on codes of conduct[3], the code of conduct of CISPE ("CISPE Code" or "Code") was reviewed by the French Supervisory Authority as the Competent Supervisory Authority (hereinafter the "CompSA").

2. The CISPE Code has been reviewed according to the procedures set up by the EDPB.

3. The FR SA has submitted its draft decision regarding the draft CISPE Code, requesting an opinion of the EDPB pursuant to Article 64(1)(b) GDPR on 29 February 2021. The decision on the completeness of the file was taken on 31 March 2021.

2 ASSESSMENT

2.1 The Code of conduct meets the needs of the sector

2.1.1 Presentation of the sector

4. Cloud computing consists of a set of technologies and service models that focus on the Internet-based use and delivery of IT applications, processing capability, storage and memory space.

5. The CISPE Code aims to contribute to the proper application of the GDPR, taking into account the specific features of the cloud computing sector.

6. The term "cloud computing" covers a variety of very distinct service provision models such as Cloud Infrastructure as a Service Cloud ("IaaS"), Cloud Software as a Service ("SaaS") and Cloud Platform as a Service ("PaaS"). The term "IaaS" describes a situation in which a provider leases a technological infrastructure, i.e. virtual remote servers the end-user can rely upon in accordance with mechanisms and arrangements such as to make it simple, effective as well as beneficial to replace the corporate IT systems at the company's premises and/or use the leased infrastructure alongside the corporate systems. When providing "SaaS", a provider delivers, via the web, various application services and makes them available to end-users. These services are often meant to replace conventional applications to be installed by users on their local systems; accordingly, users are ultimately meant to outsource their data to the individual provider. When providing "PaaS", a provider offers solutions for

[3] Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/676 adopted by the EDPB on 4 June 2019.

the advanced development and hosting of applications. These services are usually addressed to market players that use them to develop and host proprietary application-based solutions to meet in-house requirements and/or to provide services to third parties.

2.1.2 The code owner as a representative organisation

7. Codes of conduct must be submitted for approval to the supervisory authority which is competent in accordance with article 55 of the GDPR. In case of transnational codes, when identifying the competent SA, some factors could be taken into account, for example, the location of the largest density of the processing activity or the location of the code owner's headquarters.[4]

8. The Cloud Infrastructure Service Providers (CISPE) is a non-profit association established in Belgium.

9. The code owner has identified the French supervisory authority as the competent supervisory authority for the purposes of seeking approval of the CISPE Code. The code owner has justified his choice in the code of conduct based on several criteria such as the establishment of several CISPE members in France or the establishment of officers of CISPE including the treasurer and the chairman's companies in France.

10. In accordance with Article 40 (2) GDPR, a code of conduct has to be prepared by associations or others bodies representing categories of controllers or processors (code owners). Because the code owner has a major role in ensuring consistency and harmonization of practices within the sector concerned by the code, it has to demonstrate to the CompSA that it is an effective representative organization. As such, as stated in the Guidelines, the code owner should be capable of understanding the needs of their members and define the processing activity or sector to which the code is intended to apply.[5]

11. Recital 99 GDPR advises to consult during the process of drawing up a Code of Conduct with relevant stakeholders. The CISPE Code has been prepared through a collaborative process between the CISPE members, all of whom are cloud infrastructure service providers (hereinafter "CISPs") providing cloud infrastructure services to European customers. CISPE is intended to represent CISPs and includes representatives from market leading CISPs offering services throughout Europe, across many EU member states. All relevant stakeholders have been consulted and asked to approve the CISPE code of conduct. In this way, the Code provides a summary of stakeholder's consultations.

12. The code owner has demonstrated in the draft Code that it is an effective representative body, capable of understanding the needs of their members.

2.1.3 Processing Scope

13. The CISPE Code applies to the specific features of processing by IaaS providers. It seeks to bring clarity as to what GDPR means in practice when applied to IaaS providers, and what are the actual measures which CISPs will take to ensure compliance with GDPR. The Code requirements set out the GDPR principles which CISPs, as data processors, must respect. It therefore does not apply to "business to consumer" (B2C) services or for any processing activities for which the CISP may act as a data controller. However, the code is also relevant for consumers who will get additional guarantees of compliance when entrusting with their personal data a company which uses a processor which adheres to the Code.[6]

[4] See Appendix 2 to the Guidelines.
[5] See para. 22 Guidelines.
[6] It shall be noted, that the adherence of a processor to the Code of Conduct does not entail an automatic recognition of compliance of the processing carried out by such processor nor waives the responsibility of the

2.1.4 Territorial scope

14. The scope of the CISPE Code is transnational and is intended to apply across the EEA, as per article 40 (7) GDPR. The CISPE Code has identified all European Union and European Economic Area supervisory authorities as concerned SAs.

2.2 The code of conduct facilitates the effective application of the GDPR

15. The Guidelines precise that Codes will need to specify the practical application of the GDPR and accurately reflect the nature of the processing activity or sector. They should be able to provide clear industry specific improvements in terms of compliance with data protection law. A code shall not just re-state the GDPR. Instead, it should aim to codify how compliance to GDPR can be achieved in a specific, practical and precise manner.[7] Furthermore, the code has to provide sufficient appropriate safeguards to mitigate the risk around data processing and the right and freedoms of individuals.[8]

16. The CISPE Code contains both strict requirements particularizing the provisions of the GDPR mentioned in the "Processing Scope" section of the present Opinion and good practices currently followed by the sector. The CISPE Code helps CISPs to understand clearly what their obligations are under the GDPR, facilitates best practice compliance by IaaS providers and improves upon the state of the art for data protection in the Cloud sector

2.2.1 The code as a practical tool

17. The Code seeks to bring clarity as to what GDPR means in practice when applied to IaaS providers, and what are the actual measures which CISPs will take to ensure compliance with GDPR. The CISPE Code describes the rights and obligations of adhering CISPs on the basis of key principles of GDPR such as purpose limitations, data subject rights, transfers, security, auditing, liability, etc.

2.2.2 Matrix of requirements

18. The Code consists of a set of requirements that CISPs have to implement to comply with the Code.

19. The Codes develops requirements which are unambiguous, concrete, attainable and enforceable. All the requirements are consolidated in a control framework, which ensures transparency for all Code's members and data subjects and facilitates its application and interpretation, enabling implementation, monitoring and where required auditing. The EDPB welcomes the use of this kind of tool.

2.2.3 Binding nature of the Code

20. All provisions of the Code are binding, wherever the provisions make use of "shall", "must". Some provisions should be regarded as guidance, setting examples of good practices and are denoted by the use of the terms "should" or "may".

2.2.4 The Code provides sufficient safeguards

21. In line with the Guidelines,[9] a code of conduct must provide sufficient safeguards while being adequately focused on particular data protection areas and issues in the specific sector to which it applies ("added value"). The CISPE Code provides sufficient safeguards by, for instance adopting the same terminology as the one used in the GDPR and providing complaint mechanism to data subjects. In terms of added value, the code provides guidance adapted to the sector on, among others, security measures, auditing requirements, data subject rights and transparency requirement.

2.2.5 The Code as an accountability tool

22. The objective of the CISPE Code is to help CISPs to demonstrate compliance with article 28 GDPR and make it easier and more transparent for customers to analyze whether cloud services are appropriate for their use case in line with article 28.1 GDPR which provides that controllers shall use only processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject and article 28.5 GDPR which states that the adherence of a processor to an approved code of conduct may be used as an element by which to demonstrate sufficient guarantees as referred to in paragraphs 1 and 4 of article 28 GDPR.

2.3 The code of conduct provides effective mechanisms for monitoring compliance with a code

23. As per Article 40(4) of the GDPR and the Guidelines,[10] a code requires the implementation of suitable mechanisms to ensure that its rules are appropriately monitored and that efficient and meaningful enforcement measures are put in place to ensure full compliance. A code specifically needs to identify and propose structures and procedures which provide for effective monitoring and enforcement of infringements.

2.3.1 Adherence to the Code

24. The code has to detail an adhesion mechanism.

25. An effective adhesion mechanism has to develop a process divided on three phases which coincide with the code of conduct "lifetime". During the first phase, the mechanism must precise that the code members must comply with all the Code requirements and that the monitoring body will assess the eligibility of candidate to the code. In a second phase, the mechanism shall describe how that monitoring is carried out on an ongoing basis and in a third phase on ad hoc basis.[11] The CISPE Code develops an adhesion mechanism which fulfills the three phases of monitoring.

2.3.2 The monitoring of the Code

26. The Guidelines indicate that a code will also need to identify an appropriate body which has at its disposal mechanisms to enable that body to provide for the effective monitoring of compliance with the code.[12] As per Article 41 (1) GDPR, the monitoring body identified by the Code has to be accredited by the CompSA[13] Consequently, the CompSA will act as a single point of contact with the code owner and the monitoring body.

27. The CISPE Code has appointed several external monitoring bodies in accordance with article 41 of the GDPR. These monitoring bodies will be in charge of ensuring compliance of the members of the Code with the provisions of the CISPE Code and taking actions including sanctions in case of infringement to

controller to ensure compliance for all the processing operations carried out on its behalf. In this particular case, the EDPB recalls that the Code of Conduct won't apply to all the processing operations carried out on behalf of the controller, but only to the elements of Article 28 GDPR and related relevant articles. In addition, it shall be recalled that, in this case, the monitoring of the CISPE Code of Conduct is based on a service-level approach. Thus, members of the Code might not adhere to the Code with regard to all the elements of all their processing activities, but they can declare which of their services are to be considered compliant with the Code.

[7] Para 36-37 of the Guidelines.

[8] Para 39 of the Guidelines.

[9] See para 36 of the Guidelines.

[10] See para 40 of the Guidelines.

[11] Para 70 of the Guidelines.

[12] Para 40 of the Guidelines.

[13] In accordance with the consistency mechanism referred to in Article 63 of the GDPR, the EDPB adopted an Opinion 3/2020 on the France data protection supervisory authority draft accreditation requirements for a code of conduct monitoring body pursuant to article 41 GDPR on 28 January 2020. The monitoring bodies designated by the code owner of the CISPE code of conduct will have to be accredited by the French SA and therefore will have to demonstrate that they fulfil the requirements imposed by article 41 of the GDPR.

the provisions of the CISPE Code. Decisions taken by these monitoring bodies relating to their monitoring functions (for instance regarding the interpretation of the Code's rules) shall not be submitted to another entity for approval. Indeed, these monitoring bodies have to be independent in their mission.

28. The EDPB acknowledges that the CISPE Code contains a mechanism which enables the monitoring bodies to carry out their monitoring functions, as per article 40 (4) of the GDPR.

29. Finally, the EDPB recalls that the code of conduct will not be operational before the designated monitoring body is accredited.[14]

2.3.3 Sanctions

30. In accordance with article 40 (4) of the GDPR and the Guidelines, without prejudice to the tasks and powers of the competent supervisory authority, the monitoring body designated by the code owner shall, subject to appropriate safeguards, take appropriate action in cases of infringement of the code by a controller or processor. Those sanctions range from non-public but formal reprimand to temporary or permanent revocation from the Code. The monitoring body commits to inform the competent supervisory authority about any related actions taken.

31. To ensure transparency to code members, the code shall include a list of corrective measures which must be applied by the monitoring body. For this purpose, the CISPE Code develops an enforcement framework which determines the appropriate sanction to be followed by the monitoring bodies.

2.3.4 The review of the code

32. As per article 40 (2) of the GDPR and the Guidelines, the code sets out an appropriate review mechanism to ensure that the code remains relevant to legal and technical standard. In particular, section 7.3 of the CISPE Code provides that a regular review of the Code to reflect legal, technological or operational changes and best practices shall take place when appropriate.

3 CONCLUSIONS / RECOMMENDATIONS

33. By way of conclusion, the EDPB considers that the draft code complies with the GDPR, since the CISPE code of conduct fulfills the requirements imposed by Article 40 and 41 GDPR.

34. Finally, the EDPB also recalls the provisions contained within Article 40 (5) GDPR, in case of amendment or extension of the CISPE code of conduct, the CompSA will have to submit the modified version to the EDPB in accordance with the procedures outlines in the guidelines approved by the EDPB.

4 FINAL REMARKS

35. This opinion is addressed to the FR SA and will be made public pursuant to Article 64(5)(b) GDPR.

36. According to Article 64(7) and (8) GDPR, the FR SA shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.

37. Pursuant to Article 70(1)(y) GDPR, the FR SA shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.

[14] Where several monitoring bodies are designated by the code, the accreditation of one of them is sufficient to provide to the code of conduct a binding nature.

38. As per Article 40 (8) GDPR, the Board shall submit this opinion to the European Commission.

For the European Data Protection Board

The Chair

(Andrea Jelinek)



Opinion 16/2021 on the draft decision of the Belgian Supervisory Authority regarding the "EU Data Protection Code of Conduct for Cloud Service Providers" submitted by Scope Europe

Adopted on 19 May 2021

Table of contents

1 SUMMARY OF THE FACTS....4
2 ASSESSMENT....4
2.1 The Code of conduct meets the needs of the sector....4
2.1.1 Presentation of the sector....4
2.1.2 The code owner as a representative organisation....5
2.1.3 Processing Scope....5
2.1.4 Territorial scope....6
2.2 The code of conduct facilitates the effective application of the GDPR....6
2.2.1 The code as a practical tool....6
2.2.2 Matrix of requirements....6
2.2.3 Binding nature of the Code....7
2.2.4 The Code provides sufficient safeguards and added value....7
2.2.5 The Code as an accountability tool....7
2.3 The code of conduct provides effective mechanisms for monitoring compliance with a code 7
2.3.1 Adherence to the Code....7
2.3.2 The monitoring of the Code....8
2.3.3 Sanctions....8
2.3.4 The review of the code....8
3 CONCLUSIONS / RECOMMENDATIONS....9
4 FINAL REMARKS....9

The European Data Protection Board

Having regard to Article 63, Article 64(1)(b) and Article 40 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter "GDPR"),

Having regard to the European Economic Area (hereinafter "EEA") Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018[1],

Having regard to Articles 10 and 22 of its Rules of Procedure.

Whereas:

(1) Member States, Supervisory Authorities, the European Data Protection Board and the European Commission shall encourage the drawing up of codes of conduct (hereinafter "code") to contribute to the proper application of the GDPR[2].

(2) The main role of the European Data Protection Board (hereinafter "the EDPB") is to ensure the consistent application of the GDPR when a supervisory authority (hereinafter "SA") intends to approve a code of conduct that related to processing activities in several Member States (hereinafter "transnational code") pursuant to Article 40.7 GDPR and to the Board's "Guidelines 1/2019 on Codes of Conduct and Monitoring bodies under Regulation 2016/679" (hereinafter the "Guidelines").

(3) The EDPB welcomes and acknowledges the efforts made by the associations and others bodies representing categories of controllers or processors to elaborate codes of conduct which are practical and potentially cost effective tools to ensure greater consistency among a sector and foster the right to privacy and data protection of data subjects by increasing transparency.

(4) This opinion aims to ensure the consistent application of the GDPR, including by the SAs, controllers and processors and to highlight the core elements which each code of conduct has to develop.

(5) Taking into account the specific characteristics of the sector concerned, each code of conduct should be addressed individually and is without prejudice of the assessment of any other code of conduct. The EDPB recalls that Codes represent an opportunity to establish a set of rules which contribute to the proper application of the GDPR in a practical, transparent and potentially cost-effective manner that takes on board the specificities for a particular sector and/or its processing activities.

(6) The EDPB underlines that codes of conduct are voluntary accountability tools, and that the adherence to a code does not prevent SAs from exercising their enforcement power and prerogatives.

(7) The present code is not a code of conduct according to Article 46(2)(e) meant for international transfers of personal data and therefore does not provide appropriate safeguards within the framework of transfers of personal data to third countries or international organisations under the terms referred to in point (e) of Article 46 (2). Indeed, any transfer of personal data to a third country or to an international organisation, shall take place only if the provisions of chapter V of the GDPR are respected.

(8) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in guidelines on codes of conduct[3], the "EU Data Protection Code of Conduct for Cloud Service Providers" ("EU Cloud Code" or "Code") was reviewed by the Belgian Supervisory Authority as the Competent Supervisory Authority (hereinafter the "CompSA").

2. The EU Cloud Code has been reviewed according to the procedures set up by the EDPB.

3. The BE SA has submitted its draft decision regarding the EU Cloud Code, requesting an opinion of the EDPB pursuant to Article 64(1)(b) GDPR on 29 February 2021. The decision on the completeness of the file was taken on 31 March 2021.

2 ASSESSMENT

2.1 The Code of conduct meets the needs of the sector

2.1.1 Presentation of the sector

4. Cloud computing consists of a set of technologies and service models that focus on the Internet-based use and delivery of IT applications, processing capability, storage and memory space.

5. The EU Cloud Code aims to contribute to the proper application of the GDPR, taking into account the specific features of the cloud computing sector.

6. The term "cloud computing" covers a variety of very distinct service provision models such as Cloud Infrastructure as a Service Cloud ("IaaS"), Cloud Software as a Service ("SaaS") and Cloud Platform as a Service ("PaaS"). The term "IaaS" describes a situation in which a provider leases a technological infrastructure, i.e. virtual remote servers the end-user can rely upon in accordance with mechanisms and arrangements such as to make it simple, effective as well as beneficial to replace the corporate IT systems at the company's premises and/or use the leased infrastructure alongside the corporate systems. When providing "SaaS", a provider delivers, via the web, various application services and makes them available to end-users. These services are often meant to replace conventional applications to be installed by users on their local systems; accordingly, users are ultimately meant to outsource their data to the individual provider. When providing "PaaS", a provider offers solutions for the advanced development and hosting of applications. These services are usually addressed to market

[1] References to "Member States" made throughout this opinion should be understood as references to "EEA Member States".
[2] Article 40(1) of the GDPR.

[3] Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/676 adopted by the EDPB on 4 June 2019.

players that use them to develop and host proprietary application-based solutions to meet in-house requirements and/or to provide services to third parties.

2.1.2 The code owner as a representative organisation

7. Codes of conduct must be submitted for approval to the supervisory authority which is competent in accordance with Article 55 of the GDPR. In case of transnational codes, when identifying the competent SA, some factors could be taken into account, for example, the location of the largest density of the processing activity or the location of the code owner's headquarters. [4]

8. The EU Cloud Code owner is "Scope Europe" a non-profit association established in Belgium.

9. The code owner has identified the Belgian supervisory authority as the competent supervisory authority for the purposes of seeking approval of the Eu Cloud Code. The code owner has justified its choice in the code of conduct based on the fact that the code owner's and monitoring body's headquarters are based in Belgium.

10. In accordance with Article 40 (2) GDPR, a code of conduct has to be prepared by associations or others bodies representing categories of controllers or processors (code owners). Because the code owner plays a major role in ensuring consistency and harmonization of practices within the sector concerned by the code, it has to demonstrate to the CompSA that it is an effective representative organization. As such, as stated in the Guidelines, the code owner should be capable of understanding the needs of their members and define the processing activity or sector to which the code is intended to apply. [5]

11. Recital 99 GDPR advises to consult during the process of drawing up a Code of Conduct with relevant stakeholders. A group of representatives from European and multinational cloud providers and customers, technical and legal experts, public administrations and others[6], developed a first foundation of the Code and safeguarded the involvement of different stakeholders and interest groups from early on. The Code was handed over to the EU Cloud Code General Assembly in February 2017.

12. The EU Cloud Code represents several organizations including cloud service providers and associations representing cloud service providers which constitute the General Assembly of the EU Cloud Code.

13. The code owner has demonstrated in the draft code that it is an effective representative body, capable of understanding the needs of their members.

2.1.3 Processing Scope

14. The main objective of the EU Cloud Code is to concretize the legal requirements of Art. 28 GDPR and the relevant related articles of the GDPR. The EU Cloud Code is intended to address all service types of the cloud market (e.g. IaaS, PaaS, SaaS) and creates a "baseline for implementation of GDPR" for these services. Its purpose is to provide practical guidance and define specific requirements for the cloud service providers ("CSPs").

15. The EU Cloud Code only applies to cloud services where the CSP is acting as a processor. It therefore does not apply to "business to consumer" (B2C) services or for any processing activities for which the CSP may act as a data controller. However, the Code is also relevant for consumers who will get additional guarantees of compliance when entrusting with their personal data a company which uses a processor which adheres to the Code. [7]

2.1.4 Territorial scope

16. The scope of the EU Cloud Code is transnational and is intended to apply across the EEA, as per Article 40 (7) GDPR. Scope Europe has identified all European Union and European Economic Area supervisory authorities as concerned SAs.

2.2 The code of conduct facilitates the effective application of the GDPR

17. The EDPB Guidelines precise that Codes will need to specify the practical application of the GDPR and accurately reflect the nature of the processing activity or sector. They should be able to provide clear industry specific improvements in terms of compliance with data protection law. A code shall not just re-state the GDPR. Instead, it should aim to codify how compliance with the GDPR can be achieved in a specific, practical and precise manner. [8] Furthermore, the code has to provide sufficient appropriate safeguards to mitigate the risk around data processing and the right and freedoms of individuals. [9]

18. The EU Cloud Code contains both strict requirements particularizing the provisions of the GDPR mentioned in the "Processing Scope" section of the present Opinion and good practices currently followed by the sector. The Code aims to create comparability between different data processing practices in the cloud industry and improves upon the state of the art for data protection in this sector.

2.2.1 The code as a practical tool

19. The EU Cloud Code aims for all service types of the cloud market (e.g. IaaS, PaaS, SaaS) to concretize the legal requirements of Art. 28 GDPR and the relevant related articles of the GDPR. The Code describes the rights and obligations of adhering CSPs on key principles of GDPR such as purpose limitations, data subject rights, transfers, security, auditing, liability, etc.

2.2.2 Matrix of requirements

20. The Code consists of a set of requirements that CSPs have to implement to comply with the Code.

21. Those requirements are supported by a "controls catalogue" helping to assess compliance with the requirements of the Code. The "controls catalogue" maps the requirements of the Code to auditable elements ("controls"), and also maps requirements of the Code to corresponding provisions of the GDPR and relevant international standards, thus facilitating its application and interpretation and enabling implementation, monitoring and where required auditing.

22. The "controls" are to be read in conjunction with the "control guidance" which give advice on how to implement the "controls".

[4] See Appendix 2 to the Guidelines.
[5] See para 22 of the Guidelines.
[6] CSIG – Cloud Select Industry Group - https://ec.europa.eu/digital-single-market/en/news/cloud-select-industry-group-csig-plenary-meeting.

[7] It shall be noted, that the adherence of a processor to the Code of Conduct does not entail an automatic recognition of compliance of the processing carried out by such processor nor waives the responsibility of the controller to ensure compliance for all the processing operations carried out on its behalf. In this particular case, the EDPB recalls that the Code of Conduct won't apply to all the processing operations carried out on behalf of the controller, but only to the elements of Article 28 GDPR and related relevant articles. In addition, it shall be recalled that, in this case, the monitoring of the EU Cloud Code of Conduct is based on a service-level approach. Thus, members of the Code are not expected to adhere to the Code with regard to all the elements of all their processing activities, but they can declare which of their services are to be considered compliant with the Code.
[8] Para 36-37 of the Guidelines.
[9] Para 39 of the Guidelines.

23. The Code develops requirements which are unambiguous, concrete, attainable and enforceable. All the requirements are consolidated in a control framework, which ensures transparency for all Code's members and data subjects. The EDPB welcomes the use of this kind of tool.

2.2.3 Binding nature of the Code

24. All provisions of the Code and the "controls catalogue" are binding, wherever the provisions make use of "shall", "must". Some provisions should be regarded as guidance, setting examples of good practices and are denoted by the use of the terms "should" or "may".

2.2.4 The Code provides sufficient safeguards and added value

25. In line with the Guidelines[10], a code of conduct must provide sufficient safeguards while being adequately focused on particular data protection areas and issues in the specific sector to which it applies ("added value"). The EU Cloud Code provides sufficient safeguards by, for instance adopting the same terminology as the one used in the GDPR (Code, section 2) and providing complaint mechanism to data subjects (Code, section 7.8.2). In terms of added value, the Code provides guidance adapted to the sector on, among others, security measures, auditing requirements, data subject rights and transparency requirement.

2.2.5 The Code as an accountability tool

26. The objective of the EU Cloud Code is to help CSPs to demonstrate compliance with Article 28 GDPR and make it easier and more transparent for customers to analyze whether cloud services are appropriate for their use case in line with Article 28.1 GDPR, which provides that controllers shall use only processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject, and Article 28.5 GDPR which states that the adherence of a processor to an approved code of conduct may be used as an element by which to demonstrate sufficient guarantees as referred to in paragraphs 1 and 4 of Article 28 GDPR.

2.3 The code of conduct provides effective mechanisms for monitoring compliance with a code

27. As per Article 40(4) of the GDPR and the Guidelines,[11] a code requires the implementation of suitable mechanisms to ensure that its rules are appropriately monitored and that efficient and meaningful enforcement measures are put in place to ensure full compliance. A code specifically needs to identify and propose structures and procedures which provide for effective monitoring and enforcement of infringements

2.3.1 Adherence to the Code

28. The code has to detail an adhesion mechanism.

29. An effective adhesion mechanism has to develop a process divided on three phases which coincide with the code of conduct "lifetime". During the first phase, the mechanism must precise that the code members must comply with all the Code requirements and that the monitoring body will assess the eligibility of candidate to the code. In a second phase, the mechanism shall describe how that monitoring is carried out on an ongoing basis and in a third phase on ad hoc basis.[12] The EU Cloud Code develops an adhesion mechanism which fulfills the three phases of monitoring.

[10] Para 36 of the Guidelines.
[11] See para 40 of the Guidelines.
[12] See para 70 of the Guidelines.

2.3.2 The monitoring of the Code

30. The Guidelines indicate that a code will need to identify an appropriate body which has at its disposal mechanisms to enable that body to provide for the effective monitoring of compliance with the code.[13] As per Article 41 (1) GDPR, The monitoring body identified by the Code has to be accredited by the CompSA[14]. Consequently, the CompSA will act as a single point of contact with the code owner and the monitoring body.

31. The EU Cloud Code has appointed "Scope Europe" as monitoring body in accordance with Article 41 of the GDPR. This monitoring body will be in charge of ensuring compliance of the members of the Code with the provisions of the EU Cloud Code and taking actions including sanctions in case of infringement to the provisions of the EU Cloud Code. Decisions taken by the monitoring body relating to its monitoring function (for instance regarding the interpretation of the Code's rules) shall not be submitted to another entity for approval. Indeed, the monitoring body has to be independent in its mission.

32. The EDPB acknowledges that the EU Cloud Code contains a mechanism which enables the monitoring body to carry out its monitoring functions, as per article 40 (4) of the GDPR.

33. Finally, the EDPB recalls that the code of conduct will not be operational before the designated monitoring body is accredited

2.3.3 Sanctions

34. In accordance with article 40 (4) of the GDPR and the Guidelines, without prejudice to the tasks and powers of the competent supervisory authority, the monitoring body designated by the code owner shall, subject to appropriate safeguards, take appropriate action in cases of infringement of the code by a controller or processor. Those sanctions range from non-public but formal reprimand to temporary or permanent revocation from the Code. The monitoring body commits to inform the competent supervisory authority about any related actions taken (Code, section 7.9).

35. To ensure transparency to code members, the code shall include a list of corrective measures which must be applied by the monitoring body. For this purpose, the EU Cloud Code develops an enforcement framework which determines the appropriate sanction to be followed by the monitoring body (Code, section 7.9).

2.3.4 The review of the code

36. As per Article 40 (2) of the GDPR and the Guidelines, the code sets out an appropriate review mechanism to ensure that the code remains relevant to legal and technical standards. In particular, section 8.2 of the EU Cloud Code provides that a regular review of the Code to reflect legal, technological or operational changes and best practices shall take place when appropriate.

[13] See para 40 of the Guidelines.
[14] In accordance with the consistency mechanism referred to in Article 63 of the GDPR, the EDPB adopted an Opinion 2/2020 on the Belgium data protection supervisory authority draft accreditation requirements for a code of conduct monitoring body pursuant to article 41 GDP on 28 January 2020. The monitoring body designated by the code owner of the EU Cloud Code will have to be accredited by the Belgian SA and therefore will have to demonstrate that it fulfills the requirements imposed by article 41 of the GDPR.

3 CONCLUSIONS / RECOMMENDATIONS

37. By way of conclusion, the EDPB considers that the draft code complies with the GDPR, since the EU Cloud Code fulfills the requirements imposed by Article 40 and 41 GDPR.

38. Finally, the EDPB also recalls the provisions contained within Article 40 (5) GDPR, in case of amendment or extension of the EU Cloud Code, the CompSA will have to submit the modified version to the EDPB in accordance with the procedures outlined in the Guidelines approved by the EDPB.

4 FINAL REMARKS

39. This opinion is addressed to the BE SA and will be made public pursuant to Article 64(5)(b) GDPR.

40. According to Article 64(7) and (8) GDPR, BE SA shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.

41. Pursuant to Article 70(1)(y) GDPR, the BE SA shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.

42. As per Article 40 (8) GDPR, the Board shall submit this opinion to the European Commission.

For the European Data Protection Board

The Chair

(Andrea Jelinek)



Opinion 15/2021 regarding the European Commission Draft Implementing Decision pursuant to Directive (EU) 2016/680 on the adequate protection of personal data in the United Kingdom

Adopted on 13 April 2021

CONTENTS

1 EXECUTIVE SUMMARY ... 3
2 INTRODUCTION ... 5
2.1 UK data protection framework ... 5
2.2 Scope of the EDPB's assessment ... 5
2.3 General comments and concerns ... 7
2.3.1 International commitments entered into by the UK ... 7
2.3.2 Possible future divergence of UK Data Protection Framework ... 7
3 RULES APPLYING TO THE PROCESSING OF PERSONAL DATA BY COMPETENT AUTHORITIES FOR THE CRIMINAL LAW ENFORCEMENT PURPOSES ... 8
3.1 Material scope ... 8
3.2 Safeguards, rights and obligations ... 9
3.2.1 Processing on the basis of "consent" of the data subject ... 9
3.2.2 Individual rights ... 10
3.2.2.1 National security certificates ... 10
3.2.2.2 LED Automated decision-making ... 11
3.2.3 Onward transfers ... 11
3.2.4 Further processing, including onward sharing for national security purposes ... 13
3.3 Oversight and enforcement ... 14

The European Data Protection Board

Having regard to Article 51(1)(g) of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA[1] (hereinafter "LED"),

Having regard to Article 12 and Article 22 of its Rules of Procedure,

HAS ADOPTED THE FOLLOWING OPINION:

1 EXECUTIVE SUMMARY

1. The European Commission endorsed its draft implementing decision (hereinafter "draft decision") on the adequate protection of personal data by the United Kingdom (hereinafter "UK") pursuant to the LED on 19 February 2021[2]. Following this, the European Commission initiated the procedure for its formal adoption.

2. On the same date, the European Commission asked for the opinion of the European Data Protection Board (hereinafter "EDPB")[3]. The EDPB's assessment of the adequacy of the level of protection afforded in the UK has been made on the basis of the examination of the draft decision itself, as well as on the basis of an analysis of the documentation made available by the European Commission.

3. The EDPB has used as main reference for this work its LED Adequacy Referential[4] adopted on 2 February 2021, as well as the relevant case-law reflected in the EPDB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures[5].

4. The EDPB's key objective is to give an opinion to the European Commission on the adequacy of the level of protection afforded to individuals in the UK. It is important to recognise that the EDPB does not expect the UK legal framework to replicate European data protection law.

5. However, the EDPB recalls that, to be considered as providing an adequate level of protection, Article 36 LED and the case-law of the Court of Justice of the European Union (hereinafter "CJEU") require the third country's legislation to be aligned with the essence of the fundamental principles enshrined in the LED. In the area of data protection, the EDPB notes that there is a strong alignment between the LED framework and the UK legal framework on certain core provisions such as, for example concepts (e.g., "personal data"; "processing of personal data"; "data controller"); grounds for lawful and fair processing for legitimate purposes; purpose limitation; data quality and proportionality; data

[1] OJ L 119, 4.5.2016, p. 89.
[2] See European Commission's press Release, press release, Data protection: European Commission launches process on personal data flows to UK, 19 February 2021, https://ec.europa.eu/commission/presscorner/detail/en/ip_21_661.
[3] Idem.
[4] See EDPB Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive, adopted on 2 February 2021, https://edpb.europa.eu/sites/edpb/files/files/file1/recommendations012021onart.36led.pdf_en.pdf.
[5] See EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, adopted on 10 November 2020, https://edpb.europa.eu/our-work-tools/our-documents/preporki/recommendations-022020-european-essential-guarantees_en.

retention, security and confidentiality; transparency; special categories of data; automated decision making and profiling.

6. The EDPB recommends that the European Commission complement its analysis with information about the existence of a mechanism to inform the relevant Member States' competent authorities of further processing or disclosure by the UK authorities to which they transferred the personal data and identify its effectiveness under the UK legal order.

7. The EDPB considers that the provisions under Chapter 5 of Part 3 Data Protection Act 2018 (hereinafter "DPA 2018"), do, in principle, provide for a level of protection that is essentially equivalent to the one guaranteed under EU law, when it comes to transfer of personal data from a UK law enforcement authority to a third country.

8. Although the EDPB notes the capacity of the UK, under its legal framework, to recognise territories as providing an adequate level of data protection in light of the UK data protection framework, the EDPB wishes to highlight that this might lead to possible risks in the protection provided to personal data transferred from the EU especially if, in the future, the UK data protection framework deviates from the EU acquis. **For the above situations, the European Commission should therefore fulfil its monitoring role, and in case the essentially equivalent level of protection of personal data transferred from the EU is not maintained, the European Commission should consider amending the adequacy decision to introduce specific safeguards for data transferred from the EU, and/or to suspend the adequacy decision.**

9. **Finally, regarding international agreements concluded between the UK and third countries,** the European Commission is invited to examine the interplay between the UK data protection framework and its international commitments, in particular to ensure the continuity of the level of protection where personal data are transferred from the EU to the UK on the basis of the UK adequacy decision, and then onward transferred to other third countries; and to continuously monitor and take action, where necessary, in the event that the conclusion of international agreements between the UK and third countries risks to undermine the level of protection of personal data provided for in the EU.

10. In this regard, the EDPB highlights that the entry into force of the Agreement between the UK and the US on Access to Electronic Data for the Purpose of Countering Serious Crime (hereinafter "UK-US CLOUD Act Agreement")[6] may affect onward transfers from law enforcement authorities in the UK, in particular in relation to the issuance and transmission of orders as per Article 5 of the UK-US CLOUD Act Agreement.

11. The EDPB also recommends that the European Commission continuously monitors whether the conclusion of future agreements with third countries for the purpose of law enforcement cooperation, providing a legal basis for the transfer of personal data to these countries, could affect the conditions for onward sharing of the information collected, in particular whether the provisions of these international agreements may affect the application of UK data protection law and provide for further limitation or exemption in relation to the further use and disclosure overseas of information collected for law enforcement purposes. The EDPB considers that such information and assessment are essential in order to allow a comprehensive review of the level of protection afforded by the UK legislative framework and practices in relation to overseas disclosure.

[6] See Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime, Washington DC, USA, 3 October 2019.

2 INTRODUCTION

2.1 UK data protection framework

12. The UK data protection framework is largely based on the EU data protection framework (in particular the LED and Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter "GDPR")), which derives from the fact that the UK was a Member State of the EU up until the 31 January 2020. Moreover, the DPA 2018, which came into force on 23 May 2018 and repealed the UK Data Protection Act 1998, transposes the LED through Part 3 thereof, in addition to further specifying the application of the GDPR in UK law, as well as granting powers and imposing duties on the national data protection supervisory authority, the UK Information Commissioner's Office (hereinafter "ICO").

13. As mentioned in recital 12 of the draft decision, the UK Government enacted the European Union (Withdrawal) Act 2018, which incorporates directly applicable EU legislation into the law of the UK. Under this Act, the ministers of the UK have the power to introduce secondary legislation, via statutory instruments, to make the necessary modifications to retained EU law following to the UK's withdrawal from the EU to fit the domestic context.

14. Consequently, the relevant legal framework applicable in the UK after the end of the transition period[7] consists of:

- the United Kingdom General Data Protection Regulation (hereinafter "UK GDPR"), as incorporated into the law of the UK under the European Union (Withdrawal) Act 2018, as amended by the DPPEC (Data Protection, Privacy and Electronic Communications (Amendment Etc.) (EU Exit)) Regulations 2019;
- the DPA 2018, as amended by the DPPEC Regulations 2019, and the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020; and
- the Investigatory Power Act 2016 ("IPA 2016").

(together "the UK Data Protection Framework").

2.2 Scope of the EDPB's assessment

15. The draft decision of the European Commission is the result of an assessment of the UK data protection framework, followed by discussions with the UK Government. In accordance with Article 51(1)(g) LED, the EDPB is expected to provide an independent opinion on the European Commission's findings, identify insufficiencies in the adequacy framework, if any, and endeavour to make proposals to address these.

16. As mentioned in the LED Adequacy Referential, "*the information provided by the European Commission should be exhaustive and put the EDPB in a position to make an own assessment regarding the level of data protection in the third country*[8]".

[7] The transition period is set for 31 December 2020 after which date EU law no longer applies in the UK. The "bridge period" is set for 30 June 2021 at the latest and refers to the additional period during which transmission of personal data from the EU to the UK is not deemed a transfer.
[8] See Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive, para 15, p. 5.

17. In this regard, it is to be noted that the EDPB only partially received documents relevant for the examination of the UK legal framework on time. The EDPB received most part of the UK legislation referred to in the draft decision through links referenced in the latter. The European Commission was not in a position to provide the EDPB with written explanations and commitments from the UK in relation to the exchanges between the UK authorities and the European Commission relevant to this exercise[9].

18. Taking into account the above and due to the limited timeframe (2 months) afforded to the EDPB to adopt this opinion, the EDPB has chosen to focus on some specific points presented in the draft decision and provide its analysis and opinion on them. When analysing the law and practice of a third country which has been a Member State of the EU until recently, it is evident that the EDPB has identified many aspects to be essentially equivalent. In view of its role in the process of adopting an adequacy finding and the amount of law and practice to be analysed, the EDPB has decided to focus its attention to those aspects where it saw the greatest need to look closer.

19. The EDPB took into account the applicable European data protection framework, including Articles 7, 8 and 47 of the Charter of Fundamental rights of the European Union (hereinafter "the EU Charter"), respectively protecting the right to private and family life, the right to protection of personal data, and the right to an effective remedy and fair trial; and Article 8 of the European Convention on Human Rights (hereinafter "ECHR") protecting the right to private and family life. In addition to the above, the EDPB considered the requirements of the LED, as well as the relevant case-law.

20. The objective of this exercise is to provide the European Commission with an opinion for the assessment of the adequacy of the level of protection in the UK. The concept of "adequate level of protection", which already existed under Directive 95/46/EC, has been further developed by the CJEU. It is important to recall the standard set by the CJEU in *Schrems I*, namely that – while the "level of protection" in the third country must be "essentially equivalent" to that guaranteed in the EU – "the means to which that third country has recourse, in this connection, for the purpose of such a level of protection may differ from those employed within the EU"[10]. Therefore, the objective is not to mirror point by point the European legislation, but to establish the essential and core requirements of the legislation under examination. Adequacy can be achieved through a combination of rights for the data subjects and obligations on those who process data, or who exercise control over such processing and supervision by independent bodies. However, data protection rules are only effective if they are enforceable and followed in practice. It is therefore necessary to consider not only the content of the rules applicable to personal data transferred to a third country or an international organisation, but also the system in place to ensure the effectiveness of such rules. Efficient enforcement mechanisms are of paramount importance to the effectiveness of data protection rules[11].

[9] These are the elements where the European Commission refers, in its draft decision, to explanations from the UK authorities without providing the written documents from the UK authorities supporting the explanations, such as with regard to: the effects of the transitional provisions and the absence of a "sunset" provision (recital 87); examples of consent as an appropriate basis for the processing (footnote 68); the term "inaccurate" as "incorrect or misleading" personal data (footnote 79); the remit of ISC (footnote 245); the low threshold for making a complaint with the IPT and the fact that it is not unusual for the IPT to determine that the complainant was in fact never subject to investigation by a public authority (footnote 263); the combination of powers derived from the legislation and common law (footnote 52); the prerogative powers exercised by the government (footnote 62); the fact that other organisations are free to follow the MoPI Code of Practice principles if they wish (footnote 86).

[10] See CJEU, C-362/14, *Maximilian Schrems v Data Protection Commissioner*, 6 October 2015, ECLI:EU:C:2015:650 (hereinafter "*Schrems I*"), paras. 73-74.

2.3 General comments and concerns

2.3.1 International commitments entered into by the UK

21. According to Article 36 (2) (c) LED and the LED Adequacy Referential[12], when assessing the adequacy of the level of protection of a third country, the European Commission shall take into account, among others, the international commitments the third country has entered into, or other obligations arising from the third country's participation in multilateral or regional systems in particular in relation to the protection of personal data, as well as the implementation of such obligations. Furthermore, the third country's accession to the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to the Automatic Processing of Personal Data (hereinafter "Convention 108")[13] and its Additional Protocol[14] should be taken into account.

22. **In this regard, the EDPB welcomes that the UK has adhered to the ECHR and is under the jurisdiction of the European Court of Human Rights ("ECtHR"). In addition, the UK has also adhered to Convention 108 and its Additional Protocol, has signed Convention 108+[15] in 2018 and is currently working on its ratification.**

2.3.2 Possible future divergence of UK Data Protection Framework

23. As mentioned in recital 171 of the draft decision, the European Commission must take into account that, with the end of the transition period provided by the Withdrawal Agreement[16], the UK administers, applies and enforces its own data protection regime and as soon as the bridge provision[17] under Article FINPROV.10A of the EU-UK Trade and Cooperation Agreement[18] ceases to apply, this may notably involve amendments or changes to the data protection framework assessed in the draft decision, as well as other relevant developments.

[11] See EDPB Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive, para. 14, p. 5.

[12] See EDPB Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive, para 24, p. 7.

[13] See Convention for the protection of individuals with regard to the processing of personal data, Convention 108, 28 January 1981.

[14] See Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows, opened for signature on 8 November 2001.

[15] See Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (hereinafter "Convention 108+"), 18 May 2018.

[16] See Agreement on the withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community (OJ L 029, 31.1.2020, p. 7).

[17] The transition period is set for 31 December 2020, after which date EU law no longer applies in the UK. The "Bridge period" is set for 30 June 2021 at the latest, and refers to the additional period during which transmission of personal data from the EU to the UK is not deemed a transfer.

[18] See Trade and cooperation agreement between the European union and the European atomic energy community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part (OJ L 444, 31.12.2020, p. 14).

24. The European Commission has therefore decided to include a sunset clause in its draft decision[19], setting the expiration date four years after its entry into force.

25. It is important to note that the possibility of the UK ministers and the UK Secretary of State to introduce secondary legislation following the end of the bridge period may lead to a significant divergence of the UK Data Protection Framework from the EU's in the future.

26. Finally, not only since the end of the transition period, the UK is no longer bound by CJEU case-law but also, the already adopted judgments of the CJEU, considered as retained case law in the UK legal framework, might not bind the UK any more as, in particular, the UK has the possibility to modify retained EU law after the end of the bridge period and its Supreme Court is not bound by any retained EU case-law[20].

27. **Considering the risks related to the possible deviation of the UK Data Protection Framework from the EU acquis following the end of the bridge period, the EDPB welcomes the European Commission's decision to introduce a sunset clause of four years for the draft decision. However, the EDPB would like to highlight here the importance of the European Commission's monitoring role[21]. Indeed, the European Commission should monitor all relevant developments in the UK that may have an impact on the essential equivalence of the level of protection of personal data transferred under the UK adequacy decision on an ongoing and permanent basis from its entry into force. In addition, the European Commission should take appropriate action by suspending, amending or repealing the adequacy decision, based on the circumstances at hand, if after the adequacy decision is adopted, the European Commission has indications that an adequate level of protection is no longer ensured in the UK.**

28. On its side, the EDPB will use its best efforts to inform the European Commission about any relevant action undertaken by Member State's Data Protection Supervisory Authorities (hereinafter "SAs"), and in particular regarding complaints made by data subjects in the EU concerning the transfer of personal data from the EU to the UK.

3 RULES APPLYING TO THE PROCESSING OF PERSONAL DATA BY COMPETENT AUTHORITIES FOR THE CRIMINAL LAW ENFORCEMENT PURPOSES

3.1 Material scope

29. In relation to recitals 24 and following of the draft decision, the EDPB notes that the draft adequacy decision does not contain much details on the activities and legal framework applicable to agencies other than the police having law enforcement duties.

30. For example, the UK Explanatory Framework for Adequacy Discussions, Section F: Law Enforcement[22], suggests on page 11 that **the National Crime Agency** (hereinafter "NCA") could be a law enforcement agency of particular interest, which *inter alia* has a wider criminal intelligence function. The NCA describes its mission as bringing together intelligence from a range of sources in order to maximise analysis, assessment and tactical opportunities, including from technical interception of communications, law enforcement partners in the UK and overseas, security and intelligence agencies[23]. The NCA is also one of the main interlocutors for the international law enforcement partners and plays a key role in the exchange of criminal intelligence[24].

31. The EDPB further takes note of the fact that the Government Communications Headquarters (hereinafter "GCHQ"), whose activities typically fall under the scope of Part 4 DPA 2018, i.e. national security, assumes as well an active role in reducing the societal and financial harm which serious and organised crime causes to the UK, working closely with the Home Office, NCA, HM Revenue and Customs ("HMRC"), and other government departments[25]. Its activities relate to countering child sexual abuse, fraud, other types of economic crime, including money laundering, criminal use of technology, cybercrime, organised immigration crime, including people trafficking, and drugs, firearms and other illicit smuggling activity.

32. **The EDPB calls on the European Commission to complement its analysis with an analysis of the agencies active in the field of law enforcement that seem to have made collecting and analysing data, including personal data a focus of their day-to-day operations, in particular the NCA. In addition, the EDPB invites the Commission to have a closer look into the agencies like the GCHQ, whose activities fall both within the scope of law enforcement and national security, and the legal framework applicable to them for the processing of personal data.**

3.2 Safeguards, rights and obligations

3.2.1 Processing on the basis of "consent" of the data subject

33. The EDPB takes note that the European Commission asserts in recitals 37 and 38 of the draft decision that **the reliance on consent** is not considered relevant in an adequacy scenario, as in transfer situations the data are not directly collected from a data subject by a UK law enforcement authority on the basis of consent.

[19] See Article 4 of the draft decision. See also recital 172 of the draft decision.
[20] See section 6(3) to (6) EU (Withdrawal) Act 2018.
[21] See Article 36(4) LED.
[22] See UK Government, Explanatory Framework for Adequacy Discussions, Section F: Law Enforcement, 13 March 2020. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872237/F_-_Law_Enforcement_.pdf.
[23] See National Crime Agency's website, Intelligence: enhancing the picture of serious organised crime affecting the UK, https://www.nationalcrimeagency.gov.uk/what-we-do/how-we-work/intelligence-enhancing-the-picture-of-serious-organised-crime-affecting-the-uk.
[24] While not all intelligence processed by the NCA is personal data, a substantial portion might be personal information and the activities here described differ from those of classic policing, so that an assessment of access to personal data by law enforcement in the UK would be incomplete without thoroughly assessing the activities of the NCA. It seems reasonable to make sure that data protection principles are awarded the same meaning across all relevant law enforcement agencies, therefore shedding light on an especially data-driven agency such as the NCA. In addition, in "looking to the future", the explanation continues, "[w]e continuously look for new opportunities to collect, develop and enhance traditional capabilities to increase the quantity and quality of intelligence available to exploit both in the UK and abroad." "As part of this we are developing the new National Data Exploitation Capability, using the powers vested in the agency by the Crime and Courts Act, to link together, access and exploit data held across government." [...] "All of this will increase our agility and flexibility to respond to new threats and operate in a proactive way, to gather and analyse information and intelligence on emerging threats so that we can take action before threats are realised."
[25] See GCHQ's website, Mission, Serious and Organised Crime, https://www.gchq.gov.uk/section/mission/serious-crime.

34. In this regard, the EDPB recalls, that Article 36(2)a) LED requires assessing a broad array of elements not limited to the transfer situation, including "*the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including [...] criminal law*".

35. Consent in the law enforcement context can be relevant as a legal basis for data processing, as an additional safeguard, or more generally as a basis to execute investigative powers that lead to the acquisition of personal data, for example the consent of a third party to search their premises, or to confiscate data storage.

36. The EDPB notes, based also on the information provided by the European Commission in recital 38 of the draft decision, that the use of consent, as framed in the UK regime, would always require a legal basis to be relied upon. This means that even if the police have statutory powers to process the data for the purpose of an investigation, in certain specific circumstances (for example to collect a DNA sample), the police may consider appropriate to ask for the consent of the data subject.

37. **The EDPB invites the European Commission to analyse, as a rule, the possible use of consent in a law enforcement context when assessing the adequacy of a third country under the LED.**

3.2.2 Individual rights

3.2.2.1 National security certificates

38. According to section 79 DPA 2018, controllers may apply for national security certificates issued by a Minister, member of the Cabinet, the Attorney general or the Advocate General for Scotland, certifying that limitations of obligations and rights enshrined in Chapters 3 and 4 of Part 3 DPA 2018 are a necessary and proportionate measure for the protection of national security.

39. These certificates are meant to give controllers greater legal certainty, and will be conclusive evidence of the fact that national security is applicable when processing personal data. However, it should be mentioned that these certificates are not required in order to rely on national security restrictions but instead are a measure of transparency[26].

40. The EPDB understands from Schedule 20 DPA 2018, sections 17 and 18 that a national security certificate issued under the Data Protection Act 1998 (hereinafter "old certificate") had an extended effect for the processing of personal data under the DPA 2018 until 25 May 2019. Until this date, unless replaced or revoked, the old certificates were treated as if they were issued under the DPA 2018. However, where there is no express expiry date on a national security certificate issued under the Data Protection Act 1998, the EDPB understands that such a certificate will continue to have effect in relation to processing under the Data Protection Act 1998, unless the certificate is revoked or quashed.[27] Even though the protection provided by these old certificates is limited to the processing of personal data under the Data Protection Act 1998, the EDPB takes note of the fact that new national security certificates can be issued under the Data Protection Act 1998 for personal data that was processed under the Data Protection Act 1998.[28]

41. **For the sake of comprehensiveness, the EDPB invites the European Commission to clarify in its draft adequacy decision that national security certificates can still be issued under the Data Protection Act 1998. Moreover, the EDPB invites the European Commission to describe in its draft adequacy decision the redress and oversight mechanisms with regard to certificates issued under the Data Protection Act 1998. Finally, the EDPB invites the European Commission to include in its draft adequacy decision the number of existing certificates issued under the Data Protection Act 1998, and to attentively monitor this aspect.**

[26] See UK Home Office, The Data Protection Act 2018, National Security Certificates Guidance, August 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf, p. 4.
[27] See UK Home Office, The Data Protection Act 2018, National Security Certificates Guidance, August 2020, p. 5.
[28] See UK Home Office, The Data Protection Act 2018, National Security Certificates Guidance, August 2020, p. 5.

3.2.2.2 LED Automated decision-making

42. The EDPB stresses that Article 11(3) LED prohibits profiling that results in discrimination against natural persons on the basis of special categories of personal data. However, the EDPB notes that section 50 DPA 2018, which sets out the specific rules for automated decision making, foresees no such prohibition.

43. **The EDPB, therefore, invites the European Commission to verify this point, and explicitly state its findings in its adequacy decision. Moreover, the EDPB invites the European Commission to closely monitor cases related to automated decision making and profiling.**

44. According to the LED Adequacy Referential, "*[t]he third country law should, in any case, provide for necessary safeguards for the data subject's rights and freedoms. In this regard, the existence of a mechanism to inform the relevant Member State's competent authorities of any further processing such as the use of the transferred data for large scale profiling, should also be taken into account*"[29].

45. **The EDPB invites the Commission to assess this element in light of the guidance given by the EDPB in its referential.**

3.2.3 Onward transfers

46. According to the LED Adequacy Referential, onward transfers of personal data by the initial recipient to another third country or international organisation must not undermine the level of protection, provided for in the Union, of natural persons whose data is transferred. Therefore, such onward data transfers should be permitted only where the continuity of the level of protection afforded under EU law is ensured. The EDPB considers that, as pointed out by the European Commission in its assessment, the provisions under Chapter 5 of Part 3 DPA 2018, and in particular section 73, do in principle provide for a level of protection that is essentially equivalent to the one guaranteed under EU law, when it comes to transfer of personal data from a UK law enforcement authority to a third country.

47. First, section 73(1)(b) DPA 2018 notably provides that a controller may not transfer personal data to a third country or to an international organisation unless "*in a case where the personal data was originally transmitted or otherwise made available to the controller or another competent authority by a member State other than the United Kingdom, that member State, or any person based in that member State which is a competent authority for the purposes of the Law Enforcement Directive, has authorised the transfer in accordance with the law of the member State.*" Such provisions appear to be in line with the LED Adequacy Referential, which provides that the existence of a mechanism for the relevant Member State's competent authorities to be informed and authorise such onward transfer of data has also to be taken into account. The initial recipient of the data transferred from the EU should be liable and be able to prove that the relevant competent authority of the Member State has authorised the onward transfer, and that appropriate safeguards are provided for onward transfers of data in the absence of an adequacy decision concerning the third country to which the data would be

[29] See EDPB Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive, paras 59-61.

onward transferred. "*In this context, the existence of an obligation or a commitment to implement relevant handling codes defined by the transferring Member States' authorities should be taken into account*"[30].

48. **The EDPB invites the Commission to assess this element in light of the guidance given by the EDPB in its LED Adequacy Referential.**

49. Second, as explained in recital 81 of the draft decision, the UK Secretary of State has the power to recognise a third country (or a territory or a sector within a third country), an international organisation, or a description of such a country, territory, sector, or organisation as ensuring an adequate level of protection of personal data, following consultation of the ICO[31]. When assessing the adequacy of the level of protection, the UK Secretary of State must consider the same elements that the European Commission is required to assess under Article 36(2)(a)-(c) LED, interpreted together with recital 67 LED and the retained EU case-law. This means that, when assessing the adequate level of protection of a third country, the relevant standard will be whether that third country in question ensures a level of protection "essentially equivalent" to that guaranteed within the UK. Although the EDPB notes the capacity of the UK, under the DPA 2018, to recognise territories as providing an adequate level of protection in light of the UK data protection framework, the EDPB wishes to highlight that these latter territories might not benefit, to date, from an adequacy decision issued by the European Commission recognising a level of protection "essentially equivalent" to that guaranteed in the EU. This might lead to possible risks in the protection provided to personal data transferred from the EU, especially if the UK data protection framework were to deviate from the EU acquis in the future. It is to be noted that in July 2020, the *Schrems II* CJEU landmark case[32] resulted in the invalidation of the US Privacy Shield Decision as, according to the CJEU, the US legal framework could not be considered as providing an essentially equivalent level of protection compared to the one of the EU. However, the already adopted judgments of the CJEU, considered as retained case-law in the UK legal framework, might not bind the UK anymore as, in particular, the UK has the possibility to modify retained EU law after the end of the bridge period, and its Supreme Court is not bound by any retained EU case-law[33].

50. **The EDPB therefore invites the European Commission to closely monitor the adequacy assessment process and criteria by UK authorities with regard to other third countries, in particular with respect to third countries not recognised as adequate under the LED by the EU.**

51. Where the European Commission would find that no essentially equivalent level of protection to that guaranteed within the EU, as per Article 36 LED, is ensured by the third country found adequate by the UK, **the EDPB invites the European Commission to take any and all necessary steps such as, for example, amending the UK adequacy decision to introduce specific safeguards for personal data originating from the EU, and/or to consider the suspension of the UK adequacy decision, where personal data transferred from the EU to the UK are subject to onward transfers to the third country in question on the basis of a UK adequacy regulation**.

[30] See EDPB Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive, paras 55 and 56.

[31] See section 182(2) DPA 2018. See also the Memorandum of Understanding on the role of the ICO in relation to new UK adequacy assessments, https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/03/secretary-of-state-for-the-department-for-dcms-and-the-information-commissioner-sign-memorandum-of-understanding/.

[32] See CJEU, C-311/18, *Data Protection Commissioner v. Facebook Ireland Ltd and Maximilian Schrems*, 16 July 2020, ECLI:EU:C:2020:559 (hereinafter "*Schrems II*").

[33] See section 6(3) to (6) of the EU (Withdrawal) Act 2018.

52. **Finally, in relation to the international agreements concluded, or to be concluded in the future, by the UK and the possible access, by authorities from third country(ies) party(ies) to such agreements, to personal data from the EU, the EDPB recommends that the European Commission examines the interplay between the UK data protection framework and its international commitments, in particular to ensure the continuity of the level of protection in case of onward transfers to other third countries of personal data transferred from the EU to the UK on the basis of a UK adequacy decision; and to continuously monitor and take action, where needed, with regard to the conclusion of international agreements between the UK and third countries that risk to undermine the level of protection of personal data provided for in the EU**. For example, while the European Commission has referred to the fact that the UK-US CLOUD Act Agreement[34] may affect onward transfers to the US from service providers in the UK, **the EDPB highlights that the entry into force of this agreement may also affect onward transfers from law enforcement authorities in the UK, in particular in relation to the issuance and transmission of orders as per Article 5 of the UK-US CLOUD Act Agreement.**

53. The EDPB also considers that the conclusion of future agreements with third countries for the purpose of law enforcement cooperation, providing a legal basis for the transfer of personal data to these countries, may also significantly affect the conditions for onward sharing of the information collected, since such agreements may affect the UK data protection legal framework as assessed.

54. **The EDPB therefore recommends that the European Commission continuously monitor whether the conclusion of future agreements between the UK and third countries may affect the application of UK data protection law, and provide for further limitation or exemption in relation to the onward sharing and the further use and disclosure overseas of information collected for law enforcement purposes. The EDPB considers that such information and assessment are essential in order to allow a comprehensive review of the level of protection afforded by the UK legislative framework and practices in relation to overseas disclosure.**

55. Finally, the EDPB takes note that in accordance with section 76(4)(b) DPA 2018 (Transfers on the basis of special circumstances), law enforcement authorities in the UK may transfer personal data to a third country or an international organisation when the transfer "*is necessary for the purpose of obtaining legal advice in relation to any of the law enforcement purposes*". **The EPDB stresses that Article 38 LED does not contain a corresponding provision; therefore invites the European Commission to clarify what is meant by legal advice, and what kind of personal data is exchanged in such cases.**

3.2.4 Further processing, including onward sharing for national security purposes

56. In its LED Adequacy Referential, the EDPB had pointed out that, concerning further processing or disclosure of data transferred from the EU for other purposes than law enforcement purposes, such as national security purposes, it should also be provided by law, be necessary and proportionate. As assessed by the European Commission in its draft decision, section 36(3) DPA 2018, the Digital Economy Act 2017, the Crime and Courts Act 2013, and the Serious Crime Act 2017 do provide for a clear legal framework allowing for onward sharing, providing that such onward sharing should be in compliance with the rules sets in the DPA 2018.

57. The EDPB notes that, in the context of further processing for other purposes of personal data transferred from the EU, the European Commission has not assessed whether there are any

[34] See Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime, Washington DC, USA, 3 October 2019, https://www.gov.uk/government/publications/ukusa-agreement-on-access-to-electronic-data-for-the-purpose-of-countering-serious-crime-cs-usa-no62019.

mechanisms for the UK law enforcement authorities to inform the relevant Member States' competent authorities of a possible further processing of data. However, the LED Adequacy Referential considers this as an element which has to be taken into account[35]. In addition, the existence of such mechanism to inform the relevant Member States' competent authorities of further processing of data for law enforcement purposes is also considered as an element to be taken into account under the LED Adequacy Referential[36].

58. **The EDPB thus invites the European Commission to complement its analysis with information about the existence of mechanisms for the UK law enforcement authorities to notify the relevant Member States' competent authorities of a possible further processing of data, transferred from the EU.**

59. Furthermore, with respect to the sharing of data collected by a criminal law enforcement authority with an intelligence agency for purposes of national security, the legal basis authorising such onward sharing is the Counter-terrorism Act 2008. In this regard, the EDPB notes that the scope and provisions of section 19 Counter-terrorism Act 2008 are not fully addressed in the European Commission's assessment, and may imply further use of a more broader nature, in particular as regards section 19(2) Counter-terrorism Act 2008, which provides that "*[i]information obtained by any of the intelligence services in connection with the exercise of any of its functions may be used by that service in connection with the exercise of any of its other functions*." In this regard, the EDPB underlines that when further processed or disclosed, the data should benefit from the same level of protection as when they were processed initially by the receiving competent authority.

3.3 Oversight and enforcement

60. The EDPB notes that the oversight of criminal law enforcement agencies is ensured by a combination of different Commissioners, in addition to the ICO. The draft adequacy findings mentions the Investigatory Powers Commissioner (hereinafter "IPC"), the Commissioner for the Retention and Use of Biometric Material, as well as the Surveillance Camera Commissioner. In this context, it is to be noted that the CJEU has repeatedly stressed the need for independent oversight. Of particular importance on questions of access to personal data transferred to the UK is the IPC. The understanding of the EDPB is that the IPC is a so-called "judicial commissioner", as other judicial commissioners, to be referred to in the context of national security chapter, and that those judicial commissioners enjoy the independence of judges, also when serving as commissioners. As to the office of the IPC, the European Commission explains in recital 245 of the draft decision that it functions independently as a so called "arm's length body", while being funded by the Home Office.

61. In addition, the IPC is also competent to the *ex-post* oversight of surveillance measures. It appears, however, that in this function the IPC's role is to make recommendations in cases of non-compliance, and to give notice to the data subject, if the error is serious and it is in the public interest for the person to be informed.

62. The EDPB has not found in the draft decision further indication to assess the independence of the Commissioner for the Retention and Use of Biometric Material, as well as of the Surveillance Camera Commissioner.

63. **The European Commission is invited to further assess the independence of the judicial commissioners, also in cases where the Commissioner is not (anymore) serving as a judge, as well as to assess the independence of the Commissioner for the Retention and Use of Biometric Material, and as of the Surveillance Camera Commissioner.**

[35] See EDPB Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive, para 41 and footnote 39.
[36] See EDPB Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive, para 40.



Opinion 14/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the United Kingdom

Adopted on 13 April 2021

CONTENTS

1. EXECUTIVE SUMMARY 4
1.1. Areas of convergence 5
1.2. Challenges 5
1.2.1. General 5
1.2.2. General data protection aspects 6
1.2.3. On the access by public authorities to data transferred to the UK 8
1.3. Conclusion 10
2. INTRODUCTION 10
2.1. UK data protection framework 10
2.2. Scope of the EDPB's assessment 11
2.3. General comments and concerns 12
2.3.1. International commitments entered into by the UK 13
2.3.2. Possible future divergence of the UK Data Protection Framework 13
3. GENERAL DATA PROTECTION ASPECTS 15
3.1. Content principles 15
3.1.1. Rights of access, rectification, erasure and objection 15
3.1.2. Restrictions on onward transfers 20
3.2. Procedural and Enforcement Mechanisms 27
3.2.1 Competent Independent Supervisory Authority 27
3.2.2. Existence of a data protection system ensuring a good level of compliance 28
3.2.3. The data protection system must provide support and help to data subjects in the exercise of their rights and appropriate redress mechanisms 28
4. ACCESS AND USE OF PERSONAL DATA TRANSFERRED FROM THE EU BY PUBLIC AUTHORITIES IN THE UK 29
4.1. Access and use by UK public authorities for criminal law enforcement purposes 29
4.1.1. Legal bases and applicable limitations/safeguards 29
4.1.1.1. The use of consent 29
4.1.1.2. Search warrants and production orders 29
4.1.1.3. Investigatory powers for law enforcement purposes 30
4.1.2. Further use of the information collected for law enforcement purposes (recitals 140-154) 31
4.1.2.1. Further use for other law enforcement purposes 31
4.1.2.2. Further use for other purposes than law enforcement within the UK 32
4.1.2.3. Further use in the context of onward transfers outside the UK 32

4.1.3. Oversight 32
4.2. General legal framework on data protection in the field of national security 33
4.2.1. National security certificates 33
4.2.2. Right to rectification and erasure 34
4.2.3. Exemptions for National Security 34
4.3. Access and use by UK public authorities for national security purposes 34
4.3.1. Legal bases, limitations and safeguards - Investigatory powers exercised in the context of national security 35
4.3.1.1. General remarks 35
4.3.1.2. Targeted acquisition and retention of communications data 38
4.3.1.3. Equipment interference 39
4.3.1.4. Bulk interception of data from bearers 39
4.3.1.5. Protection and safeguards for secondary data 41
4.3.1.6. Automated processing of communications data 42
4.3.1.7. Compliance risks and incompliant practices of competent Intelligence Community authorities 42
4.3.2. Further use of the information collected for national security purposes and overseas disclosure 44
4.3.2.1. Further use, overseas disclosure and the applicable legal framework in the UK 44
4.3.2.2. Overseas disclosure and intelligence sharing in the context of international cooperation 45
4.3.3. Oversight 48
4.3.4. Redress 49

The European Data Protection Board

Having regard to Article 70(1)(s) of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter "GDPR"),

Having regard to the European Economic Area (hereinafter "EEA") Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018[1],

Having regard to Article 12 and Article 22 of its Rules of Procedure,

HAS ADOPTED THE FOLLOWING OPINION:

1. EXECUTIVE SUMMARY

1. The European Commission endorsed its draft implementing decision (hereinafter "draft decision") on the adequate protection of personal data by the United Kingdom (hereinafter "UK") pursuant to the GDPR on 19 February 2021[2]. Following this, the European Commission initiated the procedure for its formal adoption.

2. On the same date, the European Commission asked for the opinion of the European Data Protection Board (hereinafter "EDPB")[3]. The EDPB's assessment of the adequacy of the level of protection afforded in the UK has been made on the basis of the examination of the draft decision itself, as well as on the basis of an analysis of the documentation made available by the European Commission.

3. The EDPB focused on the assessment of both the general GDPR aspects of the draft decision and on the access by public authorities to personal data transferred from the EEA for the purposes of law enforcement and national security, including the legal remedies available to individuals in the EEA. The EDPB also assessed whether the safeguards provided under the UK legal framework are in place and effective.

4. The EDPB has used as main reference for this work its GDPR Adequacy Referential[4] adopted in February 2018 and the EPDB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures[5].

[1] References to "Member States" made throughout this opinion should be understood as references to "EEA Member States".
[2] See European Commission's press release, Data protection: European Commission launches process on personal data flows to UK, 19 February 2021, https://ec.europa.eu/commission/presscorner/detail/en/ip_21_661.
[3] Idem.
[4] See Article 29 Working Party, Adequacy Referential, adopted on 28 November 2017, as last revised and adopted on 6 February 2018, WP254 rev.01 (endorsed by the EDPB, see https://edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines); (hereinafter "*GDPR Adequacy Referential*").
[5] See EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, adopted on 10 November 2020, https://edpb.europa.eu/our-work-tools/our-documents/preporki/recommendations-022020-european-essential-guarantees_en.

1.1. Areas of convergence

5. The EDPB's key objective is to give an opinion to the European Commission on the adequacy of the level of protection afforded to individuals in the UK. It is important to recognise that the EDPB does not expect the UK legal framework to replicate European data protection law.

6. However, the EDPB recalls that, to be considered as providing an adequate level of protection, Article 45 GDPR and the case-law of the Court of Justice of the European Union (hereinafter "CJEU") require the third country's legislation to be aligned with the essence of the fundamental principles enshrined in the GDPR. The UK data protection framework is largely based on the EU data protection framework (in particular the GDPR and Directive (EU) 2016/680 of the European Parliament and of the Council, hereinafter "EU Law Enforcement Directive" or "LED") which derives from the fact that the UK was a Member State of the EU up until 31 January 2020. Moreover, the UK Data Protection Act 2018, which came into force on 23 May 2018 and repealed the UK Data Protection Act 1998, further specifies the application of the GDPR in UK law, in addition to transposing the EU Law Enforcement Directive, as well as granting powers and imposing duties on the national data protection supervisory authority, the UK Information Commissioner's Office (hereinafter "ICO"). Therefore the EDPB recognises that the UK has mirrored, for the most part, the GDPR in its data protection framework.

7. **When analysing the law and practice of a third country which has been a Member State of the EU until recently, it is evident that the EDPB has identified many aspects to be essentially equivalent.**

8. In the area of data protection, the EDPB notes that there is a strong alignment between the GDPR framework and the UK legal framework on certain core provisions such as, for example, concepts (e.g., "personal data"; "processing of personal data"; "data controller"); grounds for lawful and fair processing for legitimate purposes; purpose limitation; data quality and proportionality; data retention, security and confidentiality; transparency; special categories of data; direct marketing; automated decision making and profiling.

1.2. Challenges

9. The United Kingdom was until recently a Member State of the EU; therefore, when analysing its law and practice, the EDPB has identified many aspects to be essentially equivalent. At the same time, in view of its role in the process of adopting an adequacy finding but also the time constraints, the EDPB has decided to focus its attention to those aspects where it considers that there is a need for closer look and more detailed scrutiny.

10. Nonetheless, challenges remain and the EDPB considers the following items should be further assessed to ensure that the essentially equivalent level of protection is met, and should be closely monitored in the UK by the European Commission.

1.2.1. General

11. The first challenge, a general one, relates to the monitoring of the evolution of the UK legal system on data protection as a whole. Indeed, the UK Government has indicated its intention to develop separate and independent policies in data protection with a possible will to diverge from EU data protection law. Such political declarations have not materialised yet in the UK legal framework. However, this possible future **divergence might create risks for the maintenance of the level of protection provided to personal data transferred from the EU. Therefore, the European Commission is invited to closely monitor such evolutions from the entry into force of its adequacy decision and take necessary actions including by amending and/or suspending the decision if necessary.**

1.2.2. General data protection aspects

12. First, the so-called '**immigration exemption**', laid down under **Schedule 2 to the Data Protection Act 2018, Part 1**, paragraph 4, **is 'broadly' formulated**. In particular, it also applies in case personal data are not collected for the purpose of immigration control by a controller, but are made available by the latter to another controller who processes such personal data for the purpose of immigration control.

13. The EDPB invites the European Commission to verify the state of play of the proceedings *Open Rights Group & Anor, R (On the Application Of) v Secretary of State for the Home Department & Anor [2019] EWHC 2562 (Admin)* and, since this judgment is not final (*res judicata*), to verify whether it is confirmed or reviewed by the appeal judgment, taking any update in this regard into account, and specifying it in the decision. **The EDPB calls also on the European Commission to provide in the adequacy decision further information on the immigration exemption[6], in particular in relation to the necessity and proportionality of such broad exemption in UK law, notably having regard to the broad scope of application *ratione personae*.** At the same time, the EDPB invites the European Commission to further explore whether additional safeguards exist in the UK legal framework or could be envisaged, for instance through legally binding instruments that would complement the immigration exemption by enhancing its foreseeability and the safeguards for the data subjects, also allowing for a better and prompt assessment and monitoring of the necessity and proportionality requirements.

14. Second, although the EDPB recognises that the UK has mirrored, for the most part, Chapter V GDPR in its data protection framework, the EDPB has identified certain aspects of the UK legal framework **with regard to onward transfers** that might undermine the level of protection of personal data transferred from the EEA.

15. Indeed, Article 44 GDPR[7] provides that transfers and onward transfers of personal data shall only take place if the level of protection of natural persons guaranteed by the GDPR is not undermined. **This means that not only the UK legislation shall be "essentially equivalent" to the EU legislation with regard to the processing of personal data transferred to the UK under the future adequacy decision, but also that the rules applicable in the UK with regard to the onward transfer of those data to third countries shall ensure that an essentially equivalent level of protection will continue to be provided.**

[6] Also as outcome of the ongoing review of the use of the immigration exemption referred to at p. 5 of the UK Government's Explanatory Framework for Adequacy Discussions, Section E3: Schedule 2 Restrictions, 13 March 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872232/E_-_Narrative_on_Restrictions.pdf.

[7] *"Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the Controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined."*

16. Although the EDPB notes the capacity of the UK, under its legal framework, to recognise territories as providing an adequate level of data protection in light of the UK data protection framework, the EDPB wishes to highlight that these territories might not benefit, to date, from an adequacy decision issued by the European Commission and ensure a level of protection "essentially equivalent" to that guaranteed in the EEA. This might lead to possible risks in the protection provided to personal data transferred from the EEA especially if, in the future, the UK data protection framework deviates from the EU acquis. In addition, the UK has already recognised as adequate the third countries that enjoy an adequacy finding by the European Commission under Directive 95/46/EC[8], while the European Commission will soon review these findings, and the conclusions of this review are not yet known.

17. **For the above situations, the European Commission should fulfil its monitoring role, and in case the essentially equivalent level of protection of personal data transferred from the EEA is not maintained, the European Commission should consider amending the adequacy decision to introduce specific safeguards for data transferred from the EEA and/or to suspend the adequacy decision.**

18. **Regarding international agreements concluded between the UK and third countries,** the European Commission is invited to examine the interplay between the UK data protection framework and its international commitments, beyond the Agreement on access to electronic data for the purpose of countering serious crime concluded between UK and the United States of America (hereinafter "US")[9] (hereinafter "UK-US CLOUD Act Agreement"), in particular to ensure the continuity of the level of protection where personal data are transferred from the EU to the UK on the basis of the UK adequacy decision, and then onward transferred to other third countries; and to continuously monitor and take action, where necessary, in the event that the conclusion of international agreements between the UK and third countries risks to undermine the level of protection of personal data provided for in the EU.

19. Furthermore, the European Commission is invited to monitor whether the UK-US CLOUD Act Agreement ensures appropriate additional safeguards, taking into account the level of sensitivity of the categories of data concerned and the sole requirements of the transfer of electronic evidence directly by service providers rather than between authorities, also assessing under which circumstances safeguards may be provided by an appropriate implementation of the adaptation of the EU-US Umbrella Agreement[10].

20. Further, the EDPB notes that onward transfers can also take place from the UK to another third country based on **transfer tools pursuant to the UK applicable data protection legislation**[11]. Following *Schrems II*[12], the EDPB invites the European Commission to provide reassurances in the adequacy decision that necessary safeguards will be effectively put in place taking also into account the legislation of the receiving third country.

21. Concerning the absence **of protections provided under Article 48 GDPR** in the UK legislation, the EDPB invites the European Commission to provide further assurances and specific references to the UK legislation that ensure that the level of protection under the UK legal framework is essentially equivalent to the level of protection guaranteed in the EEA.

22. With regard to **procedural and enforcement mechanisms,** the EDPB notes that the existence and effective functioning of an independent supervisory authority; the existence of a system ensuring a good level of compliance; and a system of access to appropriate redress mechanisms equipping individuals in the EEA with the means to exercise their rights and seek redress without encountering cumbersome barriers to administrative and judicial redress are key elements a data protection framework consistent with the European one must be characterized by.

23. The EDPB acknowledges that the UK has mirrored in most parts the relevant provisions of the GDPR in the UK GDPR and in the Data Protection Act 2018; nevertheless, the European Commission is invited to continuously monitor any developments in the UK legal framework and practice, which might lead to detrimental impacts on those areas.

1.2.3. On the access by public authorities to data transferred to the UK

24. The EDPB notes the significant changes in the UK legal framework applicable to security and intelligence agencies, especially regarding the interception and acquisition of communication data. The EDPB understands that these changes are, *inter alia*, a response to the proceedings initiated before the CJEU and the European Court on Human Rights (hereinafter "ECtHR") and their recent judgments in this context.

25. In particular, the EDPB welcomes the fact that the UK has established the Investigatory Powers Tribunal (hereinafter "IPT"). The IPT is not only competent to hear cases on the use of investigatory powers by law enforcement authorities, but also by intelligence services. It is therefore the understanding of the EDPB that the IPT functions as a proper court in the meaning of Article 47 Charter of Fundamental Rights of the European Union (hereinafter "EU Charter").

26. Furthermore, the EDPB positively notes the introduction of "Judicial Commissioners" in the Investigatory Powers Act 2016 (hereinafter "IPA 2016") as a significant improvement. It understands that an important function of the Judicial Commissioners is to approve *ex ante* in individual cases different surveillance measures, including targeted interception and bulk acquisition of communication data (so-called "double lock" procedure).

27. However, in order to assess the effectiveness of this additional level of oversight, the EDPB sees the need to further clarification of the scenarios for which a lawful interception without approval by the Investigatory Powers Commissioner (hereinafter "IPC") or the Judicial Commissioners is possible, and invites the European Commission to further assess and demonstrate that, even in cases where the double-lock procedure does not apply, the UK legal framework provides for appropriate safeguards, including through effective *ex post* oversight and redress possibilities offered to individuals, thus ensuring a level of protection which is essentially equivalent to the one provided within the EU.

28. Furthermore, the EDPB invites the European Commission to further assess the conditions under which urgency can be invoked, and provide clarifications concerning the possible avenues for the exercise of rights for the data subjects concerned and possible redress avenues offered to them in

[8] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).
[9] See Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime, Washington DC, USA, 3 October 2019, https://www.gov.uk/government/publications/ukusa-agreement-on-access-to-electronic-data-for-the-purpose-of-countering-serious-crime-cs-usa-no62019.
[10] See Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences, December 2016 (hereinafter "EU-US Umbrella Agreement"), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3A3104_8.
[11] See Articles 46 and 47 UK GDPR.
[12] See *Schrems II*.

the context of equipment interference operations, especially in the case of a derogation to the double-lock procedure.

29. In addition, the EDPB considers that there is a need for further clarification and assessment of bulk interceptions, in particular on the selection and application of the selectors, in order to clarify the extent to which access to personal data meets the threshold set by the CJEU, and which safeguards are in place to protect the fundamental rights of individuals whose data are intercepted in this context, including concerning the retention periods of data. An independent assessment from competent UK oversight authorities would be particularly useful. The EDPB also underlines that it seems all the more critical that "overseas-related communications" which are within the scope of bulk interception practices appear to imply that data could be directly intercepted and collected in bulk within the EU by the UK, including for data in transit between the EU and the UK, which would fall within the scope of the draft decision. Given the importance of this aspect, the EDPB calls on the European Commission to closely monitor developments in this regard.

30. Still in relation to bulk interception, the EDPB stresses the consistent assessment by the ECtHR and the CJEU, and recalls the concerns expressed in relation to secondary data, which should benefit from specific safeguards due to their sensitivity. The EDPB therefore calls on the European Commission to carefully assess whether the safeguards provided under UK law for such category of personal data ensure an essentially equivalent level of protection to the one guaranteed in the EEA.

31. In this context, the EDPB is aware of the fact that the 2016 Intelligence and Security Committee's public report concerning the use of bulk powers[13] concerns practices under the previous legal framework, which was subsequently replaced by the IPA 2016. Nevertheless, it sees a need for further independent assessment and oversight of the use of automated processing tools by the competent UK oversight authorities, and calls on the European Commission to further assess this issue and the safeguards that would and/or could be afforded to EEA data subjects in this context.

32. The EDPB shares the view expressed by the IPC that further review and monitoring are needed to ensure that the safeguards, applied in practice by competent authorities in the field of national security and intelligence to remedy incompliances with the application of the relevant legislation, are maintained and will continue to be improved. The EDPB also welcomes the fact that consequently, the IPC conducted a review of its approach to inspecting bulk interception in 2019, "*which included a careful review of the technically complex ways in which bulk interception is actually implemented*" and committed to include "*a detailed examination of the selectors and search criteria alluded to above by the ECtHR*" in the inspections of bulk interception from 2020 onwards. Given the importance of this aspect, the EDPB is concerned that detailed examination of the selectors and search criteria has not been carried out yet by the IPC, and calls on the European Commission to closely monitor developments in this regard, especially since the concrete format of such oversight remains to be clarified.

33. The EDPB underlines that, when it comes to overseas disclosures, the application of national security exemption provided under UK law may lead to the absence of safeguards ensuring that the principles of purpose limitation, necessity and proportionality would also be respected or foreseeing that sufficient rights of the individuals, oversight and redress would also be provided or respected in the third country of destination. The EDPB therefore recommends the European Commission to further

[13] See Report of the bulk powers review, by the Independent Reviewer of Terrorism Legislation, August 2016, https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2016/08/Bulk-Powers-Review-final-report.pdf.

examine the overall safeguards provided under UK law when it comes to overseas disclosure, in particular in light of the application of national security exemptions.

34. Finally, the EDPB is concerned about other forms of information sharing and disclosures, on the basis of other instruments, in particular the various international agreements concluded by the UK with other third countries, especially where these instruments remain inaccessible to the public, such as the UK-US Communication Intelligence Agreement. The effect of such agreement could lead to a circumvention of the safeguards identified in relation to the access and use of personal data for national security purposes. The EDPB considers that the conclusion of bilateral or multilateral agreements with third countries for the purpose of intelligence cooperation, providing a legal basis for direct interception and acquisition of personal data or the transfer of personal data to these countries may also significantly affect the conditions for further use of the information collected, since such agreements are likely to affect the UK data protection legal framework as assessed.

1.3. Conclusion

35. The EDPB considers that the UK adequacy assessment is unique because of the previous status of the UK as an EU Member State. Besides, it would also be the first adequacy decision including a sunset clause.

36. Accordingly, the EDPB recognises many areas of convergence between the UK and the EU data protection frameworks. At the same time, however, and following a careful analysis of the European Commission's draft decision and the UK data protection legislation, the EDPB has identified a number of challenges, which are examined extensively in this opinion. In this context, the EDPB wishes to emphasise the paramount role of the European Commission on the monitoring of all relevant developments in the UK.

37. In light of the above, the EDPB recommends the European Commission to address the challenges raised in this opinion. The EDPB also invites the European Commission to monitor closely all relevant developments in the UK that may have an impact on the essential equivalence of the level of protection of personal data, and to take swiftly appropriate actions, where necessary.

2. INTRODUCTION

2.1. UK data protection framework

38. The UK data protection framework is largely based on the EU data protection framework (in particular the GDPR and the LED), which derives from the fact that the UK was a Member State of the EU up until 31 January 2020. Moreover, the UK Data Protection Act 2018, which came into force on 23 May 2018 and repealed the UK Data Protection Act 1998, further specifies the application of the GDPR in UK law, in addition to transposing the EU Law Enforcement Directive, as well as granting powers and imposing duties on the national data protection supervisory authority, the UK ICO.

39. As mentioned in recital 12 of the European Commission's draft decision, the UK Government enacted the European Union (Withdrawal) Act 2018, which incorporates directly applicable EU legislation into the law of the UK. Under this Act, the ministers of the UK have the power to introduce secondary legislation, via statutory instruments, to make the necessary modifications to retained EU law following the UK's withdrawal from the EU to fit the domestic context.

40. Consequently, the relevant legal framework applicable in the UK after the end of the transition period[14] consists of:

- the United Kingdom General Data Protection Regulation (hereinafter "UK GDPR"), as incorporated into the law of the UK under the European Union (Withdrawal) Act 2018, as amended by the DPPEC (Data Protection, Privacy and Electronic Communications (Amendment Etc.) (EU Exit)) Regulations 2019;
- the Data Protection Act 2018 (hereinafter "DPA 2018"), as amended by the DPPEC Regulations 2019, and the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020; and
- the IPA 2016.

(together "the UK Data Protection Framework").

2.2. Scope of the EDPB's assessment

41. The draft decision of the European Commission is the result of an assessment of the UK Data Protection Framework, followed by discussions with the UK Government. In accordance with Article 70(1)(s) GDPR, the EDPB is expected to provide an independent opinion on the European Commission's findings, identify insufficiencies in the adequacy framework, if any, and endeavour to make proposals to address these.

42. As mentioned in the GDPR Adequacy Referential: "*the information provided by the European Commission should be exhaustive and put the EDPB in a position to make an own assessment regarding the level of data protection in the third country*"[15].

43. In this regard, it is to be noted that the EDPB only partially received documents relevant for the examination of the UK legal framework on time. The EDPB received most part of the UK legislation referred to in the draft decision through links referenced in the latter. The European Commission was not in a position to provide the EDPB with written explanations and commitments from the UK in relation to the exchanges between the UK authorities and the European Commission relevant to this exercise[16].

[14] The transition period is set for 31 December 2020, after which date EU law no longer applies in the UK. The "bridge period" is set for 30 June 2021 at the latest, and refers to the additional period during which transmission of personal data from the EEA to the UK is not deemed a transfer.

[15] See WP254 rev.01, p. 3.

[16] With regard to: Article 48 GDPR (footnote 78 of the draft decision); enhanced safeguards and security measures applied by controllers when processing in the national security context (footnote 64 of the draft decision); to the requirement for the controller to consider whether there is a need to rely on the exemption on a case-by-case basis even where a national security certificate has been issued (recital 126 and footnote 172 of the draft decision); the fact that the protections of the EU-US Umbrella Agreement will apply to all personal information produced or preserved under the UK-US CLOUD Act Agreement, irrespective of the nature or type of body making the request, with regard to the details of the concrete implementation of the data protection safeguards which are still subject to discussions between the UK and the US, the confirmation that UK authorities will only let this Agreement enter into force once they are satisfied that its implementation complies with the legal obligations provided therein, including clarity with respect to compliance with the data protection standards for any data requested under this Agreement (recital 153 of the draft decision); situations where data are transferred from the EU to the UK within the scope of this draft decision, and the fact that there would always be a "British Islands connection" and any equipment interference covering such data would

44. Taking into account the above, and due to the limited timeframe (2 months) afforded to the EDPB to adopt this opinion, the EDPB has chosen to focus on some specific points presented in the draft decision and provide its analysis and opinion on them.

45. When analysing the law and practice of a third country which has been a Member State of the EU until recently, it is evident that the EDPB has identified many aspects to be essentially equivalent. In view of its role in the process of adopting an adequacy finding and the amount of law and practice to be analysed, the EDPB has decided to focus its attention to those aspects where it saw the greatest need to look closer. In addition, in line with the jurisprudence of the CJEU, a very important part of the analysis covers the legal regime of national security access to the personal data transferred to the UK, and the practice of the national security apparatus in the UK. However, it has to be borne in mind that national security is evidently an area of law and practice where the legislation of Member States is not harmonised at EU level and therefore may differ.

46. The EDPB took into account the applicable European data protection framework, including Articles 7, 8 and 47 EU Charter, respectively protecting the right to private and family life, the right to protection of personal data, and the right to an effective remedy and fair trial; and Article 8 of the European Convention on Human Rights (hereinafter "ECHR"), protecting the right to private and family life. In addition to the above, the EDPB considered the requirements of the GDPR, as well as the relevant case-law.

47. The objective of this exercise is to provide the European Commission with an opinion on the assessment of the adequacy of the level of protection in the UK. The concept of "adequate level of protection", which already existed under Directive 95/46/EC, has been further developed by the CJEU. It is important to recall the standard set by the CJEU in *Schrems I*, namely that – while the "level of protection" in the third country must be "essentially equivalent" to that guaranteed in the EU – "*the means to which that third country has recourse, in this connection, for the purpose of such a level of protection may differ from those employed within the EU*"[17]. Therefore, the objective is not to mirror point by point the European legislation, but to establish the essential and core requirements of the legislation under examination. Adequacy can be achieved through a combination of rights for the data subjects and obligations on those who process data, or who exercise control over such processing, and supervision by independent bodies. However, data protection rules are only effective if they are enforceable and followed in practice. It is therefore necessary to consider not only the content of the rules applicable to personal data transferred to a third country or an international organisation, but also the system in place to ensure the effectiveness of such rules. Efficient enforcement mechanisms are of paramount importance to the effectiveness of data protection rules[18].

2.3. General comments and concerns

therefore be subject to the mandatory warrant requirement of section 13(1) of the IPA 2016 (recital 206 of the draft decision); and the examples of operational purposes provided (recital 216 and footnote 369 of the draft decision).

[17] See CJEU, C-362/14, *Maximilian Schrems v Data Protection Commissioner*, 6 October 2015, ECLI:EU:C:2015:650 (hereinafter "*Schrems I*"), paras. 73-74.

[18] See WP254 rev.01, p.2.

2.3.1. International commitments entered into by the UK

48. According to Article 45(2)(c) GDPR and the GDPR Adequacy Referential[19], when assessing the adequacy of the level of protection of a third country, the European Commission shall take into account, among others, the international commitments the third country has entered into, or other obligations arising from the third country's participation in multilateral or regional systems, in particular in relation to the protection of personal data, as well as the implementation of such obligations. Furthermore, the third country's accession to the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to the Automatic Processing of Personal Data (hereinafter "Convention 108"),[20] and its Additional Protocol[21], should be taken into account.

49. **In this regard, the EDPB welcomes that the UK has adhered to the ECHR and is under the jurisdiction of the ECtHR. In addition, the UK has also adhered to Convention 108 and its Additional Protocol, has signed Convention 108+[22] in 2018, and is currently working on its ratification.**

2.3.2. Possible future divergence of the UK Data Protection Framework

50. As mentioned in recital 281 of the draft decision, the European Commission must take into account that, with the end of the transition period provided by the Withdrawal Agreement[23], the UK administers, applies and enforces its own data protection regime, and as soon as the bridge provision under Article FINPROV.10A of the EU-UK Trade and Cooperation Agreement[24] ceases to apply, this may notably involve amendments or changes to the data protection framework assessed in the draft decision, as well as other relevant developments.

51. The European Commission has therefore decided to include a sunset clause in its draft decision[25], setting the expiration date of four years after its entry into force.

52. It is important to note that the possibility of the UK ministers and the UK Secretary of State to introduce secondary legislation following the end of the bridge period may lead to a significant divergence of the UK Data Protection Framework from the EU's in the future.

53. Indeed, the UK Government has indicated its intention to develop separate and independent policies in data protection, which may then lead to a divergence from EU data protection law[26]. This intention encompasses the inclusion of personal data aspects in trade agreements[27], a practice that entails the risk of lowering the level of protection of personal data provided for by the UK[28].

54. Finally, not only since the end of the transition period, the UK is no longer bound by CJEU case-law but also, the already adopted judgments of the CJEU, considered as retained case law in the UK legal framework, might not bind the UK any more as, in particular, the UK has the possibility to modify retained EU law after the end of the bridge period and its Supreme Court is not bound by any retained EU case-law[29].

55. **Considering the risks related to the possible deviation of the UK Data Protection Framework from the EU acquis following the end of the bridge period, the EDPB welcomes the European Commission's decision to introduce a sunset clause of four years for the draft decision. However, the EDPB would like to highlight here the importance of the European Commission's monitoring role[30]. Indeed, the European Commission should monitor all relevant developments in the UK that may have an impact on the essential equivalence of the level of protection of personal data transferred under the UK adequacy decision on an ongoing and permanent basis from its entry into force. In addition, the European Commission should take appropriate action by suspending, amending or repealing the adequacy decision, based on the circumstances at hand, if after the adequacy decision is adopted, the European Commission has indications that an adequate level of protection is no longer ensured in the UK.**

56. On its side, the EDPB will use its best efforts to inform the European Commission about any relevant action undertaken by Member State's data protection supervisory authorities (hereinafter "SAs") either in the commercial or public sector, and in particular regarding complaints made by data subjects in the EEA concerning the transfer of personal data from the EEA to the UK.

[19] See WP254 rev.01, p.2.

[20] See Convention for the protection of individuals with regard to the processing of personal data, Convention 108, 28 January 1981.

[21] See Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows, opened for signature on 8 November 2001.

[22] See Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention 108+"), 18 May 2018.

[23] See Agreement on the withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community (OJ L 029, 31.1.2020, p. 7).

[24] See Trade and cooperation agreement between the European union and the European atomic energy community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part (OJ L 444, 31.12.2020, p. 14).

[25] See Article 4 of the draft decision. See also recital 282 of the draft decision.

[26] The UK's National Data Strategy (last updated on 9 December 2020, https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy) includes the following as one of its missions: "*Championing the international flow of data. The flow of information across borders fuels global business operations, supply chains and trade, powering growth across the world. It also plays a wider societal role. The transfer of personal data ensures people's salaries are paid, and helps them connect with loved ones from afar. And, as the coronavirus pandemic has demonstrated, sharing health data can aid vital scientific research into diseases while uniting countries in their response to global health emergencies.* ***Having left the European Union, the UK will champion the benefits that data can deliver.*** *We will promote domestic best practice and work with international partners* ***to ensure data is not inappropriately constrained by national borders and fragmented regulatory regimes*** *so that it can be used to its full potential.*" (emphasis added).

[27] Ibid: "*Facilitate cross-border data flows:* ***We will work globally to remove unnecessary barriers to international data flows. We will agree ambitious data provisions in our trade negotiations*** *and use our newly independent seat in the World Trade Organisation to influence trade rules for data for the better.* ***We will remove obstacles to international data transfers*** *which support growth and innovation, including by developing a new UK capability that delivers new and innovative mechanisms for international data transfers. We will also work with partners in the G20 to create interoperability between national data regimes to minimise friction when transferring data between different countries".* (emphasis added).

[28] See European Parliament resolution of 12 December 2017 "*Towards a digital trade strategy*" (2017/2065(INI)), Section V, in which it stressed that "*The protection of personal data is non-negotiable in [EU] trade agreements*", available at: https://www.europarl.europa.eu/doceo/document/TA-8-2017-0488_EN.pdf. See also, European Parliament resolution of 25 March 2021 on the Commission evaluation report on the implementation of the General Data Protection Regulation two years after its application, para. 28 in which it is stated: *"supports the Commission's practice of addressing data protection and personal data flows separately from trade agreements"*, https://www.europarl.europa.eu/doceo/document/TA-9-2021-0111_EN.html.

[29] See section 6(3) to (6) EU (Withdrawal) Act 2018.

[30] See Article 45(4) GDPR.

3. GENERAL DATA PROTECTION ASPECTS

3.1. Content principles

57. Chapter 3 of the GDPR Adequacy Referential is dedicated to the "Content Principles". A third country's system must contain them in order for its level of data protection to be considered essentially equivalent to the one guaranteed within the EU. The EDPB acknowledges the fact that the UK does not have a codified constitution in that there is no one single document that sets out its governing fundamental rules. However, the right to respect for private and family life (and the right to data protection as part of that right) and the right to a fair trial[31] are included in the Human Rights Act 1998, and the constitutional value of this statute has been recognised by UK courts. Indeed, the Human Rights Act 1998 incorporates the rights contained in the ECHR[32]. In addition, the Human Rights Act 1998 states very importantly that any action of public authorities must be compatible with the ECHR[33].

58. Aside from structural and formalistic differences between the UK and EU legislation, the EDPB notes, as one can expect, that the UK's approach to data protection is similar to the one in the EU resulting from the fact that the UK was a Member State of the EU up until 31 January 2020. As a result, many content principles are aligned with the GDPR's; therefore provide a level of protection essentially equivalent to the one provided by the EU. The EDPB has decided not to develop further the analysis as to those content principles that are in alignment with EU legislation, and is satisfied with the analysis provided by the European Commission in its draft decision. Such content principles are for example the following: concepts (e.g., "personal data"; "processing of personal data"; "data controller"); grounds for lawful and fair processing for legitimate purposes; purpose limitation; data quality and proportionality; data retention, security and confidentiality; transparency; special categories of data; direct marketing; automated decision making and profiling. The EDPB further notes that the UK GDPR and the DPA 2018 include content principles that go further than what is required by the GDPR Adequacy Referential and mirror the principles included in the GDPR; therefore elevating the level of protection provided for in the UK. Such content principles are for example the ones related to personal data breach notifications, the data protection officer, data protection impact assessments and data protection by design and by default.

59. However, as mentioned in the Introduction, the EDPB wishes to specifically address in this opinion certain points on which the EDPB has concerns and would like to request clarifications from the European Commission.

3.1.1. Rights of access, rectification, erasure and objection

60. The so-called 'immigration exemption', laid down under **Schedule 2 to the DPA 2018, Part 1**, paragraph 4 allows controllers involved in "immigration control" to not apply certain data subjects' rights provided by the DPA 2018 if this would be likely to "*prejudice the maintenance of effective immigration control*" or "*the investigation or detection of activities that would undermine the maintenance of effective immigration control*".

[31] See Articles 6 and 8 ECHR (Schedule 1 to the Human Rights Act 1998).
[32] For more information, see recitals 8-10 of the draft decision.
[33] See section 6 Human Rights Act 1998.

61. As acknowledged by the European Commission in its draft decision[34], and referred to in the Opinion of the LIBE Committee of the European Parliament, on the conclusion, on behalf of the EU, of the Trade and Cooperation Agreement between the EU and the UK[35], this exemption is **'broadly' formulated**. It applies to the following rights: right to be informed; right of access; right to erasure; right to restrict processing; and right to object.

62. Besides, it is important to note that this exemption also applies in case personal data are not collected for the purpose of immigration control by a controller ("controller 1"), but are however made available by the latter to another controller ("controller 2") who processes such personal data for the purpose of immigration control (e.g., the UK Home Office)[36].

63. In *Open Rights Group & Anor, R (On the Application Of) v Secretary of State for the Home Department & Anor [2019] EWHC 2562 (Admin) (03 October 2019)*, the applicants challenged the lawfulness of the immigration exemption on the ground that it was contrary to Article 23 GDPR and incompatible with the rights guaranteed by Articles 7 and 8 EU Charter relating to privacy and the protection of personal data. The High Court of England and Wales (hereinafter "High Court") considered whether the immigration exemption in paragraph 4 of Part 1 of Schedule 2 of the DPA 2018 is lawful, and concluded in favour of its lawfulness.

64. The High Court considered in particular that:

[34] See recitals 62-65 of the draft decision.
[35] In this regard, on the **broad formulation** of the immigration exemption, see Opinion of the Committee on Civil Liberties, Justice and Home Affairs on the conclusion, on behalf of the Union, of the Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the one part and the United Kingdom of Great Britain and Northern Ireland, of the other part, and of the Agreement between the European Union and United Kingdom of Great Britain and Northern Ireland concerning security procedures for exchanging and protecting classified information (2020/0382(NLE)), 5 February 2021, https://www.europarl.europa.eu/doceo/document/LIBE-AL-680848_EN.pdf, para. 10: *"recalls, in this regard, Parliament's February and June 2020 resolutions, pointing out the **general and broad exemption** for the processing of personal data for immigration purposes of the UK Data Protection Act"*, and para. 11: *"considers that the **general and broad** exemption for the processing of personal data for immigration purposes of the UK Data Protection Act [...] need to be amended before a valid adequacy decision can be granted;"*(emphasis added).
[36] See example provided in the ICO "Guide to the General Data Protection Regulation (GDPR)", v 01 January 2021, p. 307 (emphasis added): *"A private organisation (controller 1) alerts the Home Office (controller 2) to an employee who is believed to have submitted false documents to evidence their identity and qualifications to obtain a job. The employer provides the Home Office with the relevant information. The right of the individual to be informed that their personal data has been passed to the Home Office is restricted in so far as giving effect to it would be likely to prejudice the investigation.*
*The **employer is therefore under no obligation to inform the individual that their information has been passed to the Home Office**, and in turn **the Home Office** is under no obligation to provide the individual with a privacy notice informing them that it is now processing their personal data. The exemption applies to both controllers to the same extent.*
*However, the employee requests a copy of their personal data from the Home Office which is now investigating them. The **Home Office may rely on the exemption** to withhold part of their data if the disclosure would be likely to prejudice the investigation. Should the employee make a similar request to **their employer, they would also be able to apply the exemption** to the same extent."*
In other words, as clarified on p. 300: *"In the majority of cases the Home Office, or one of its agencies and contractors, will be the controller applying this exemption. However, it is important to note that the application of this exemption is not just limited to the Home Office. It may also be relevant to other controllers such as employers, universities and the police, who liaise with the Home Office on immigration matters."*

- *"[…] the Immigration Exemption is plainly a matter of "important public interest" and pursues a legitimate aim.[…]"*, para. 30;
- *"the Immigration Exemption satisfies the requirements for a measure to be "in accordance with the law. […]"*, para. 38;
- *"The Immigration Exemption may only be relied on if and to the extent that compliance with "the listed GDPR provisions" **would be likely to prejudice** the maintenance of effective immigration control or the investigation or detection of activities that would undermine the maintenance of effective immigration control. The words "would be likely to prejudice", in the context of the Data Protection Act 1998 (which preceded the DPA 2018), were interpreted to mean "a very significant and weighty chance of prejudice to the particular public interest. The degree of risk must be such that there 'may very well' be prejudice to those interests, even if the risk falls far short of being more probable than not […]."*, para. 39 (emphasis added).

65. It should be noted that this judgment is, to the EDPB's knowledge, not final and has been appealed.

66. As specified in the EDPB Guidelines on restrictions under Article 23 GDPR ("the Article 23 GDPR Guidelines")[37] *"[…] in a GDPR context, restrictions shall be **provided for in a legislative measure**, concern a **limited number of rights of data subjects and/or controller's obligations** which are listed in Article 23 of the GDPR, **respect the essence** of the fundamental rights and freedoms at issue, be a **necessary and proportionate measure** in a democratic society and safeguard one of the grounds set out in Article 23(1) of the GDPR […]".*[38]

67. The EDPB also recalls that recital 41 GDPR states that *"[w]here this Regulation refers to **a legal basis or a legislative measure**, this does not necessarily require a legislative act adopted by a parliament, without prejudice to requirements pursuant to the constitutional order of the Member State concerned. However, such a legal basis or legislative measure should be **clear and precise and its application should be foreseeable to persons subject to it**, in accordance with the case-law of the Court of Justice of the European Union […] and the European Court of Human Rights"* (emphasis added).

68. Although the ECtHR specified that "*[f]urther, as regards the words "in accordance with the law" and "prescribed by law" which appear in Articles 8 to 11 of the Convention, the [ECHR] observes that it has always understood the term "law" in its "substantive" sense, not its "formal" one; it has included both "written law", encompassing enactments of lower ranking statutes and regulatory measures taken by professional regulatory bodies under independent rule-making powers delegated to them by Parliament, and unwritten law. "Law" must be understood to include both statutory law **and judge-made "law"***"[39], the Article 23 GDPR Guidelines recall that *"[a]ccording to the CJEU case law, any **legislative measure** adopted on the basis of Article 23(1) [of the] GDPR must, in particular, **comply with the specific requirements set out in Article 23(2) of the GDPR**. Article 23(2) [of the] GDPR states that the legislative measures imposing restrictions to the rights of data subjects and the controllers' obligations shall contain, where relevant, **specific provisions about several criteria outlined below**. As a rule, all the requirements detailed below **should be included in the legislative measure** imposing restrictions under Article 23 [of the] GDPR."*[40]

69. It can be observed in this regard that **the immigration exemption** itself **does not specify the following elements referred to under Article 23(2) GDPR**:

- "the safeguards to prevent abuse or the unlawful access or transfer" (d);
- "the controller or categories of controllers" (e)[41];
- "the risks to the rights and freedoms of data subjects" (g);
- "the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction" (h).

70. The ICO's "Guide to the General Data Protection Regulation (GDPR)"[42], including a Chapter on the "immigration exemption", does provide clarifications on the immigration exemption, but **cannot** *per se* provide binding rules complementing it. Moreover, the issue of 'quality of the law' is particularly relevant given the importance of the restricted rights and the extension of the exemption[43].

[37] See EDPB Guidelines 10/2020 on restrictions under Article 23 GDPR, version 1.0, adopted on 15 December 2020, which are currently under finalisation following public consultation, https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-102020-restrictions-under-artide-23_en.

[38] See Article 23 GDPR Guidelines, para. 9, p. 5.

[39] See ECtHR, *Sanoma Uitgevers B.V. v. The Netherlands*, 14 September 2010, EC:ECHR:2010:0914JUD003822403, para. 83 (emphasis added).

[40] See Article 23 GDPR Guidelines, paras. 45 and 46, p. 11. Under Article 52(3) EU Charter, *"[i]n so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection"*. On the notion of '**provided for by law**' under Article 52(1) EU Charter, the criteria developed by the ECtHR should be used as suggested in several CJEU Advocate General's Opinions, see for example the Opinions in joined cases C-203/15 and C-698/15, *Tele2 Sverige AB*, ECLI:EU:C:2016:572, paras. 137-154, and in case C-70/10, *Scarlet Extended*, ECLI:EU:C:2011:255, paras. 88-114. Hence, reference can be made, among others, to the ECtHR ruling in *Weber and Saravia v Germany*, para. 84: *"The Court reiterates that the expression **"in accordance with the law"** within the meaning of Article 8 § 2 [of the ECHR] requires, firstly, that the impugned measure should have some basis in **domestic law**; it also refers to the **quality of the law** in question, requiring that it should be accessible to the person concerned, who must, moreover, be able to foresee its consequences for him, and compatible with the rule of law."* (emphasis added).
See also recital 41 GDPR: *"Such [a legal basis or] legislative measure should be **clear** and **precise** and its application should be **foreseeable to persons subject** to it, in accordance with the case-law of the Court of Justice of the European Union (…) and the European Court of Human Rights"* (emphasis supplied).

[41] See the aforementioned High Court case, para. 54: *"In my view there is nothing unlawful about the Immigration Exemption being available **to all data controllers** processing data for the specified purposes. As the defendants point out, without paras 4(3)–(4) the Immigration Exemption would be rendered ineffective in cases where data is obtained from third parties (such as a local authority or HM Revenue and Customs) for the purposes of maintaining effective immigration control."* (emphasis added), hence confirming the **generalised** application of the restrictions.

[42] ICO's "Guide to the General Data Protection Regulation (GDPR)", v 01 January 2021, p. 299-307.

[43] See para. 57 of the aforesaid High Court case: *"Mr Knight informs me that the Commissioner is finalising guidance on the Exemption, but it will have "statutory" status only in the sense of being issued by virtue of the Commissioner's powers under art.57(1) of the GDPR. It will have no legal status under DPA 2018."*
The rationale for the introduction of legally binding guidance supported by ICO is referred to in particular at paras. 56-60 of the judgment:
"56. Finally, I turn to the Commissioner's submission that without accompanying statutory guidance to provide safeguards as to the meaning and application of the Immigration Exemption, the exemption would not be a proportionate implementation of art.23(1) of the GDPR. Mr Knight says that supplemented by such guidance, the provision is proportionate.
57. Mr Knight informs me that the Commissioner is finalising guidance on the Exemption, but it will have "statutory" status only in the sense of being issued by virtue of the Commissioner's powers under art.57(1) of

71. *A fortiori*, the "**prejudice test**" does not set out the safeguards to prevent abuse or unlawful access or transfer, and to be implemented for instance by the Home Office.

72. In the light of all of the above, the EDPB remarks that further clarifications on the application of the immigration exemption are needed.

73. Furthermore, the EDPB remarks the lack of a legally binding instrument that clarifies the immigration exemption in view of considering whether it is essentially equivalent with Article 23 GDPR and Articles 7 and 8 EU Charter. At the same time, the EDPB considers that the necessity and proportionality of the broad scope *ratione personae* of the immigration exemption needs to be further demonstrated by the European Commission, supported by evidence.

74. **As a conclusion, the EDPB invites the European Commission to verify the state of play of the proceedings *Open Rights Group & Anor, R (On the Application Of) v Secretary of State for the Home Department & Anor [2019] EWHC 2562 (Admin)* referred to above and, since this judgment is not final (*res judicata*), to verify whether it is confirmed or reviewed by the appeal judgment, to take any update in this regard into account, and to specify it in the adequacy decision. The EDPB also calls on the European Commission to provide further information on the necessity and proportionality of the immigration exemption, in particular having regard to the broad scope of application *ratione personae*.**

the GDPR. It will have no legal status under DPA 2018. I understand also that the Home Office has produced draft internal staff guidance on the Immigration Exemption (see [22] above). In practice guidance issued by the Commissioner is influential regardless of its legal basis. However, there is no power for the Commissioner to issue "binding" guidance of the sort that the Supreme Court had in mind in the Christian Institute case (at [101] and [107]). It appears that primary legislation would be required if it were considered necessary for there to be guidance on the Immigration Exemption of the same status as the codes of practice currently provided for in ss.121–124 of DPA 2018.

58. In his argument for statutory guidance Mr Knight contends that the context in which the use of the Immigration Exemption will arise necessarily frames the concerns about the necessity and proportionality of its existence and use. He draws attention to two matters in particular in the legal context. First, personal data to which the Immigration Exemption is applied is inherently likely to involve special category data within the meaning of art.9(1) of the GDPR (i.e. data "revealing racial or ethnic origin"). Such data is identified in the GDPR because it requires a higher measure of protection (Opinion 1/15 [2019] 3 C.M.L.R. 25 at [141]). Secondly, it is a basic proposition of data protection law that the right of subject access in particular is of great importance as the gateway to being able to exercise the other rights provided to data subjects (see YS v Minister voor Immigratie, Integratie en Asiel (C-141/12) EU:C:2014:2081; [2015] 1 C.M.L.R. 18 at [44]).

59. Mr Knight identifies four points of a practical nature. First, when controllers do not explain to data subjects that they have relied upon a statutory exemption, nor provide a broad summary of the reasons why, the data subject will be unaware that the exemption has been applied, and unable to challenge it effectively as a result. Secondly, data subjects will be especially reliant on controllers to apply the exemption with care and only so far as necessary. Although any data subject is entitled to complain to the Commissioner about the application of the exemption, or to bring legal proceedings before the courts, it is likely that the data subject will be unaware of their rights and lack the funds to take legal steps, in circumstances where there is a need for prompt and accurate compliance with data protection rights. Thirdly, as an immigrant the data subject is likely to be in a vulnerable position. Fourthly, this is not an abstract issue in the light of the defendants' evidence as to the use of the Immigration Exemption (see [4] above).

60. Mr Knight suggests that there is a close parallel between the present challenge to the Immigration Exemption and the reasoning of the Court in Christian Institute [2016] UKSC 51 . As in Christian Institute , he contends, the Immigration Exemption is wide, uses undefined terms, applies a low threshold, is subject to controls not apparent on the face of the provision and applies to a very broad array of contexts and rights. Unlike Christian Institute there is no publicly available guidance, still less of a statutory status even to which regard must be had, on the Immigration Exemption."

3.1.2. Restrictions on onward transfers

76. Article 44 GDPR provides that transfers and onward transfers of personal data shall only take place if the level of protection of natural persons guaranteed by the GDPR is not undermined. Therefore, personal data transferred from the EEA to the UK based on the adequacy decision shall enjoy an essentially equivalent level of protection to the one provided under the EU data protection framework. **This means that not only the UK legislation shall be "essentially equivalent" to the EU legislation with regard to the processing of personal data transferred to the UK under the draft decision, but also that the rules applicable in the UK with regard to the onward transfer of those data to third countries shall ensure that an essentially equivalent level of protection will continue to be provided.**

77. As a result, it is important that any onward transfer from the UK to another third country of personal data from the EEA is properly protected with safeguards, or is carried out in accordance with the rules on derogations[44] to ensure the continuity of protection afforded by the EU legislation. **Indeed, if no such protection can be provided, onward transfers of EEA personal data should not take place.**

78. The EDPB recognises that the UK has mirrored, for the most part, Chapter V GDPR in the UK GDPR (Articles 44-49) and in the DPA 2018[45]. **However, the EDPB has identified certain aspects of the UK legislative framework with regard to onward transfers that might undermine the level of protection of personal data transferred from the EEA.**

79. **The first challenge** the EDPB has identified relates to the recognition by the UK, following the procedure as elaborated in the DPA 2018, of third countries, international organisations or territories[46] as adequate recipients. Indeed, onward transfers of EEA personal data may occur from the UK to other third countries, on the basis of a future possible UK adequacy regulation[47].

80. More specifically, as explained in recital 77 of the draft decision, the UK Secretary of State has the power to recognise a third country (or a territory or a sector within a third country), an international organisation, or a description of such a country, territory, sector, or organisation as ensuring an adequate level of protection of personal data, following consultation of the ICO[48]. When assessing the adequacy of the level of protection, the UK Secretary of State must consider the same elements that the European Commission is required to assess under Article 45(2)(a)-(c) GDPR, interpreted together with recital 104 GDPR and the retained EU case-law. This means that, when assessing the

[44] See Article 49 UK GDPR.
[45] See section 17A, 17B, 17C and 18 DPA 2018.
[46] See section 17A of DPA 2018 DPA 2018.
[47] The UK equivalent to an adequacy decision under the GDPR.
[48] See section 182(2) DPA 2018. See also the Memorandum of Understanding on the role of the ICO in relation to new UK adequacy assessments, https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/03/secretary-of-state-for-the-department-for-dcms-and-the-information-commissioner-sign-memorandum-of-understanding/.

adequate level of protection of a third country, the relevant standard will be whether that third country in question ensures a level of protection "essentially equivalent" to that guaranteed within the UK. Although the EDPB notes the capacity of the UK, under the UK GDPR, to recognise territories as providing an adequate level of protection in light of the UK Data Protection Framework, the EDPB wishes to highlight that these latter territories might not benefit, to date, from an adequacy decision issued by the European Commission recognising a level of protection "essentially equivalent" to that guaranteed in the EU. This might lead to possible risks in the protection provided to personal data transferred from the EEA, especially if the UK Data Protection Framework were to deviate from the EU acquis in the future. It is to be noted that in July 2020, the *Schrems II* CJEU landmark case[49] resulted in the invalidation of the US Privacy Shield Decision as, according to the CJEU, the US legal framework could not be considered as providing an essentially equivalent level of protection compared to the one of the EU. However, the already adopted judgments of the CJEU, considered as retained case-law in the UK legal framework, might not bind the UK anymore as, in particular, the UK has the possibility to modify retained EU law after the end of the bridge period, and its Supreme Court is not bound by any retained EU case law[50].

81. **The EDPB invites the European Commission to closely monitor the adequacy assessment process and criteria by UK authorities with regard to other third countries, in particular with respect to third countries not recognised as adequate under the GDPR by the EU. Where the European Commission finds that no essentially equivalent level of protection to that guaranteed within the EU is ensured by a third country found adequate by the UK, the EDPB invites the European Commission to take any and all necessary steps such as, for example, amending the UK adequacy decision to introduce specific safeguards for personal data originating from the EEA, and/or to consider the suspension of the UK adequacy decision, where personal data transferred from the EEA to the UK are subject to onward transfers to the third country in question on the basis of a UK adequacy regulation.**

82. **The second challenge** relates to the upcoming review of the already existing adequacy decisions rendered by the European Commission under Directive 95/46/EC. Following this review, the European Commission might decide that certain countries that benefited until now from an adequacy decision no longer provide for an essentially equivalent level of protection taking into account the current EU legislation and recent case-law. However, as provided for in paragraph 4, Schedule 21 DPA 2018, the UK has already recognised those countries as providing for an adequate level of protection. Even though the UK Secretary of State must conduct a review of these adequacy findings within a period of four years, the European Commission notes in its draft decision that these adequacy findings will not automatically cease to exist should the UK Secretary of State not undertake the required review within the stipulated four-year time limit[51].

83. **The EDPB invites the European Commission to monitor whether, once the EU review of the already existing adequacy decisions is finalised, a country, deemed to no longer provide for an adequate level of protection, is still considered as such by the UK. If this is the case, the EDPB invites the European Commission, based on recitals 277 – 280 of the draft decision to take any appropriate measures to remedy the situation, for example by amending the adequacy decision in order to add specific requirements for personal data originating from the EEA and/or by suspending the adequacy decision, if personal data transferred from the EEA to the UK are subject to onward transfers to the third country in question. The EDPB invites the European Commission to continue this monitoring exercise for the duration of the UK adequacy decision.**

84. **The third challenge** concerns the onward transfer of personal data from the EEA to non-adequate countries based on the transfer tools provided for in Articles 46 and 47 UK GDPR. Although the UK GDPR provides for the same transfer tools as the ones provided by the GDPR, the EDPB highlights the need to ensure that the safeguards they contain provide for an effective protection in the third country, especially in the light of the *Schrems II* judgment.

85. Following the *Schrems II* ruling, in which the CJEU reminds that the protection granted to personal data in the EU must travel with the data wherever it goes, the EDPB has already adopted initial recommendations on supplementary measures[52] to assist exporters, where required, in ensuring that data subjects are afforded a level of protection essentially equivalent to that guaranteed within the EU.

86. According to the CJEU, data exporters are responsible for verifying, on a case-by-case basis and, where appropriate, in collaboration with the data importer in the third country, if the law or practice of the third country impinges on the effectiveness of the appropriate safeguards contained in the Article 46 GDPR transfer tools[53]. Where this is the case, data exporters should implement supplementary measures that fill these gaps in the protection and bring it up to the level required by EU law.

87. **The EDPB invites the European Commission, in order to ensure continuity of protection, to introduce in the draft decision reassurances that when the transfer tools provided in Articles 46 and 47 UK GPDR are used by data exporters in the UK for onward transfers to other third countries of EEA transferred data, these data exporters assess on a case-by-case basis, the data protection framework of the third country; and if necessary, take appropriate measures to ensure the effective respect of the safeguards contained in the chosen transfer tool to ensure an essentially equivalent level of protection to that guaranteed within the EU. Without these reassurances, the EDPB stresses that that there is a risk that the essentially equivalent level of protection to the one guaranteed within the EU, will be watered down through onward transfers taking place from the UK.**

88. **The fourth challenge** relating to onward transfers concerns the international agreements concluded, or to be concluded in the future by the UK and the possible direct access, by authorities from third country(ies) party(ies) to such agreements, to personal data from the EEA. Indeed, the EDPB has strong concerns in relation to the already concluded UK-US CLOUD Act Agreement and the European Commission acknowledges this challenge, stressing that "*a possible entry into force of the Agreement may impact the level of protection assessed in this Decision*"[54]. Indeed, based on this agreement, once it enters into force, personal data transferred from the EEA to the UK under the draft decision would then be subject to the provisions of this agreement laying down conditions for direct access by US authorities, impacting the UK Data Protection Framework, including the provisions on onward transfers. As a result, the level of protection provided to the data transferred from the EEA may be

[49] See *Schrems II*.
[50] See section 6(3) to (6) EU (Withdrawal) Act 2018.
[51] See recital 82 of the draft decision.
[52] See EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, adopted on 10 November 2020, which are currently under finalisation following public consultation, https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf.
[53] See *Schrems II*, para. 134.
[54] See recital 153 of the draft decision.

substantially affected by the provisions of the agreement concluded with the US, and impact on the level of protection for such data. The EDPB notes in this context that the European Commission refers to explanations given by UK authorities in recital 153 of its draft decision, without quoting or providing any concrete written assurance or commitment, nor pointing out specific legal provisions under UK law that would give effect to such explanations.

89. The EDPB has previously raised these concerns in a letter addressed to the European Parliament dated 15 June 2020[55]. The EDPB had highlighted that based on the "*EU acquis in the field of data protection, and in particular with the GDPR and the law enforcement directive*" the EDPB has reservations as to whether the safeguards in the agreement for access to personal data in the UK would apply in certain circumstances requiring disclosure obligations to the US, as well as whether these safeguards are sufficient in light of the EU standards so as to not undermine the level of protection provided in the EU.

90. Furthermore, the provisions of the UK–US CLOUD Act Agreement may significantly affect the substantive and procedural conditions under which personal data held by controllers or processors in the UK can be directly accessed by US authorities, thus impacting on the level of protection guaranteed under UK law. To provide for a level of protection essentially equivalent to the one guaranteed under EU law, it is for example "*essential that the safeguards as per such agreement include a mandatory prior judicial authorisation, as an essential guarantee for access to metadata and content data. On the basis of its preliminary assessment, the EDPB, while noting that the agreement refers to the application of domestic law, could not identify such a clear provision in the agreement concluded between the UK and the US*"[56].

91. While the European Commission highlights that data obtained under this agreement would benefit from equivalent protections to the specific safeguards provided by the so-called "EU-US Umbrella Agreement", the EDPB has concerns as to whether the incorporation of these safeguards into the UK-US CLOUD Act Agreement by a mere reference applying on a *mutatis mutandis* basis would meet the criteria of clear, precise and accessible rules when it comes to access to personal data, or would sufficiently enshrine such safeguards to be effective and actionable under UK law.

92. **The EDPB therefore recommends that the European Commission clarifies how and based on which legal instrument equivalent protections to the specific safeguards provided by the EU-US Umbrella Agreement would be given effect and have binding character under UK law.**

93. The EDPB also notes that the provisions of the UK-US CLOUD Act Agreement, read in conjunction with section 3 US CLOUD Act[57], raises questions as to the actual application of the safeguards offered by the agreement for the access, by US law enforcement authorities, to personal data in the UK processed by providers of electronic communication service or remote computing service (hereinafter "CSPs") falling under the jurisdiction of the US. Indeed, should a CSP located in the UK be subject to US law (e.g., because it is the subsidiary of a US company), it remains to be ascertained whether US authorities would be bound to rely on the UK-US CLOUD Act Agreement to obtain that data. As the European Commission points out that *"[p]articular attention will be given to the application and adaptation of the Umbrella Agreement's protections to the specific type of transfers covered by the UK-US Agreement"*, the EDPB stresses that on the basis of its preliminary assessment,

[55] See EDPB response to MEPs Sophie in't Veld and Moritz Körner on the US-UK agreement under the US Cloud Act, adopted on 15 June 2020, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_letter_out_2020-0054-uk-usagreement.pdf.
[56] See the abovementioned EDPB letter.
[57] See US CLOUD Act, https://www.congress.gov/bill/115th-congress/senate-bill/2383/text.

it is unclear whether the safeguards enshrined in the UK-US CLOUD Act Agreement, and therefore the one provided by the EU-US Umbrella Agreement, would apply to all, if any, requests for access to data in the UK made by US authorities under the US CLOUD Act.

94. There may be other future international agreements or commitments with third countries the UK might be entering into in the future, and that would apply to personal data transferred from the EEA to the UK under the draft decision[58]. Depending on the provisions of these agreements and the application of specific safeguard clauses, these international agreements, by affecting the UK Data Protection Framework may also significantly impact on the substantive and procedural conditions for access to personal data in the UK by third country authorities. This is in particular the case for the draft second additional protocol to the Council of Europe Convention on Cybercrime (hereinafter "Budapest Convention") currently being negotiated among the parties to this Convention, which include several non-EU countries. Indeed, the draft protocol includes clauses which can be discretionally activated by the parties, for instance concerning the authorisation to grant access to content data or not. While all EU Member States would activate the clauses in compliance with EU data protection rules, no guarantee has been provided concerning the UK, which could substantially deviate from the level of protection that would then be offered within the EU. Another example of the issues presented above, is the Agreement between the UK and Japan for a Comprehensive Economic Partnership[59] ("CEPA"), the UK's first post-Brexit trade deal that entered into force on 1 January 2021[60] and that includes provisions on personal data[61]. The EDPB furthermore notes that the UK has also formally announced on 1 February 2021 its request to join the Comprehensive and Progressive Trans-Pacific Partnership ("CPTPP") which incorporates the Trans-Pacific Partnership Agreement ("TPP")[62].

95. The EDPB notes that, apart from the UK-US CLOUD Act Agreement, the international agreements mentioned above are not addressed in the draft decision.

96. **The EDPB invites the European Commission to:**

- **Examine the interplay between the UK Data Protection Framework and its international commitments, beyond the UK-US CLOUD Act Agreement, in particular to ensure the continuity of the level of protection in case of onward transfers to other third countries of personal data transferred from the EEA to the UK on the basis of a UK adequacy decision; and to continuously monitor and take action, where needed, with regard to the conclusion of other international agreements between the UK and third countries that risk to undermine the level of protection of personal data provided for in the EU.**

[58] See section 2.3.3 above.
[59] See UK/Japan: Agreement for a Comprehensive Economic Partnership [CS Japan No.1/2020], https://www.gov.uk/government/publications/ukjapan-agreement-for-a-comprehensive-economic-partnership-cs-japan-no12020.
[60] See UK Government's guidance on UK trade agreements with non-EU countries, https://www.gov.uk/guidance/uk-trade-agreements-with-non-eu-countries.
[61] Pursuant to Article 8.80 para. 5 CEPA, the parties commit to encourage the development of mechanisms to promote compatibility between their different legal approaches to (personal) data protection. Pursuant to Article 8.84, the parties commit not to prohibit or restrict the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person within the meaning of CEPA.
[62] Pursuant to Article 14.11 para. 2 TPP, each party shall allow the cross-border transfer of transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person.

- **Provide the EDPB with written commitments from UK authorities and identify specific provisions under UK law, in relation to the explanation related to the possible application and implementation of the UK-US CLOUD Act Agreement as referred to in recital 153 of the draft decision.**
- **Monitor, in this context, whether, in addition to the safeguards that could be provided by an appropriate implementation of the adaptation of the EU-US Umbrella Agreement, the UK -US CLOUD Act Agreement ensures appropriate additional safeguards to take into account the level of sensitivity of the categories of data concerned and the unique requirements of the transfer of electronic evidence directly by CSPs rather than between authorities.**
- **Assess the impact and potential risks of the provisions on personal data contained in international agreements recently signed by the UK, such as the CEPA.**

97. **The fifth challenge** identified relates to the application of derogations for the transfers of personal data to a third country. Although the available derogations under the UK GDPR are the same as the ones provided under the GDPR, it is important that the ICO applies and will continue to apply an interpretation in relation to the use of these derogations aligned with the one of the EDPB. If this is not the case, or if the UK diverges from this interpretation in the future, there would be a risk that the level of protection of data transferred from the EEA to third countries via the UK could be undermined.

98. **The EDPB invites the European Commission, as part of its monitoring task, to specifically check that the UK interpretation on the use of derogations remains aligned to the EU's interpretation. If however, a different interpretation of the use of derogations were followed by the UK undermining the level of protection, it is essential that the European Commission takes necessary steps by amending the adequacy decision to make sure that the level of protection provided to EEA personal data transferred to the UK will not then be undermined when these data are onward transferred from the UK to third countries on the basis of a different interpretation of derogations.**

99. **The sixth challenge,** final one for this section, refers to the absence of protections provided under Article 48 GDPR in the UK Data Protection Framework.

100. The European Commission indeed clarifies in its draft decision that in the absence of adequacy regulations or appropriate safeguards, a transfer can only take place based on derogations set out in Article 49 UK GDPR, "*with the exception of Article 48 of Regulation (EU) 2016/679 that the United Kingdom has chosen not to include in the UK GDPR.*"[63] The absence of an essentially equivalent provision to Article 48 GDPR enshrined in the UK Data Protection Framework, in relation to transfers or disclosures, following a judgment of a court or tribunal or a decision of an administrative authority from another third country, may give rise to legal uncertainty as to whether the level of protection for personal data transferred from the EEA to the UK under the draft decision would be substantially affected.

101. In its GDPR Adequacy Referential, the EDPB points out that, when it comes to onward transfers, "*further transfers of the personal data by the initial recipient of the original data transfer should be permitted only where the further recipient is also subject to rules affording an adequate level of protection and following the relevant instructions when processing data on the behalf of the data controller*"[64]. Furthermore, the EDPB stresses that "*the initial recipient of the data transferred from the EU shall be liable to ensure that appropriate safeguards are provided for onward transfers of data in the absence of an adequacy decision. Such onward transfers of data should only take place for limited and specified purposes and as long as there is a legal ground for that processing*"[65]. As part of Chapter V GDPR, Article 48 has to be taken fully into account in assessing whether the UK legal framework ensures an essentially equivalent level of protection in this regard[66].

102. The EDPB emphasises in this context the CJEU case-law in relation to the risk of abuse or unlawful access and use of data, stating in particular that "*as regards the level of protection of fundamental rights and freedoms that is guaranteed within the European Union, EU legislation involving interference with the fundamental rights guaranteed by Articles 7 and 8 of the Charter must, according to the Court's settled case-law, lay down clear and precise rules governing the scope and application of a measure and imposing minimum safeguards, so that the persons whose personal data is concerned have sufficient guarantees enabling their data to be effectively protected against the risk of abuse and against any unlawful access and use of that data. The need for such safeguards is all the greater where personal data is subjected to automatic processing and where there is a significant risk of unlawful access to that data*"[67].

103. The EDPB notes in this regard that, based on the information available in the draft decision, the UK Data Protection Framework does not clearly provide that any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement in force between the requesting third country and the UK. Article 48 GDPR is an essential provision under Chapter V GDPR as it requires that a transfer or disclosure of personal data following a judgment or decision from a third country court/tribunal or administrative authority may only be recognised or enforceable if based on an international agreement in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfers pursuant to Chapter V GDPR. Indeed, the EDPB recalls that "*a request from a foreign authority does not in itself constitute a legal ground for transfer. The order can only be recognised 'if based on an international agreement such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State*"[68]. It is therefore key that essentially equivalent provisions can be identified under UK law.

104. In the draft decision, the European Commission reports explanations from the UK authorities according to which under common law or statutes, a foreign judgment requesting data is unenforceable in the UK without an international agreement and any transfer of data upon request from a foreign court or administrative authority requires a transfer tool such as an adequacy regulation or appropriate safeguards, unless a derogation under Article 49 UK GDPR applies. However, the EDPB has not been provided with the exchanges between the European Commission and the UK authorities[69] in this regard, and is therefore not able to analyse and independently assess

[63] See footnote 78 of the draft decision.

[64] See WP 254 rev.01, p. 6.
[65] See WP 254 rev.01, p. 6.
[66] See Article 44 GDPR, last sentence, in particular: "*All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.*"
[67] See *Schrems I*, para. 91.
[68] See the annex to the EDPB-EDPS Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection, adopted on 10 July 2019, https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-edps-joint-response-libe-committee-impact-us-cloud-act_en.
[69] See footnote 78 of the draft decision.

whether the guarantees provided by the UK authorities are sufficient to ensure an essentially equivalent level of protection in relation to the safeguards contained in Article 48 GDPR.

105. **The EDPB invites the European Commission to provide further assurances and specific references to UK legislation that ensure that the level of protection under the UK legal framework is essentially equivalent to that guaranteed within the EEA. Therefore, the EDPB invites the European Commission to provide written explanations and commitments from the UK authorities with regard to the implementation of protections essentially equivalent to those provided by Article 48 GDPR.**

106. **The EDPB considers that the identification of provisions under UK law ensuring an essentially equivalent level of protection in relation to the safeguards contained in Article 48 GDPR is all the more important in light of the concerns previously raised concerning requests for access to data in the UK made by US or other third countries' authorities, and considering that as per the adequacy decision, personal data could be transferred from the EEA to the UK without any further guarantee or binding commitment from the recipient in relation to requests for access to data by other third countries' authorities.**

3.2. Procedural and Enforcement Mechanisms

107. Based on the criteria set forth in the GDPR Adequacy Referential, the EDPB has analysed the following aspects of the UK Data Protection Framework as covered under the draft decision: the existence and effective functioning of an independent supervisory authority; the existence of a system ensuring a good level of compliance; and a system of access to appropriate redress mechanisms equipping individuals in the EU with the means to exercise their rights and seek redress without encountering cumbersome barriers to administrative and judicial redress.

3.2.1 Competent Independent Supervisory Authority

108. The EDPB welcomes the efforts of the European Commission to examine comprehensively the establishment, functioning and powers of the UK supervisory authority in Chapter 2.6. of the draft decision. In the UK, the Information Commissioner (hereinafter "IC") is tasked with the oversight and enforcement of the compliance with the UK GDPR and the DPA 2018. According to Schedule 12 DPA 2018, the IC is a "Corporation Sole", i.e. a separate legal entity constituted in a single person, supported by an office, the ICO.

109. With regard to the independence of the IC, the EDPB underlines that Article 51 UK GDPR does not contain the express clarification that the IC is an independent public authority as it is stated in Article 51 GDPR with regard to SAs. The EDPB nevertheless acknowledges, that the UK GDPR mirrors in its Article 52 in a similar manner the corresponding rules with regard to the independence as set forth in Article 52(1) to (3) GDPR.

110. Furthermore, the EDPB points out that Article 52 UK GDPR does not hold obligations corresponding to Article 52(4) to (6) GDPR that expressly ensure that the respective SA is provided with resources necessary for the effective performance of its tasks and exercise of its powers. The EDPB however recognises that the DPA 2018 contains provisions which aim to secure an appropriate funding of the ICO[70], as well as the circumstance that the ICO is currently one of the largest SA compared to SAs within the EU/EEA. Since an ongoing allocation of appropriate resources, especially with regard to staff and budget[71], is imperative so as to ensure the proper functioning of a SA to fulfil all of its

[70] See sections 137, 138, 182 and Schedule 12 para. 9 DPA 2018.
[71] See WP 254 rev.01, p. 7.

assigned tasks and it has also been recently flagged by the European Parliament to be of major importance[72], the EDPB deems it essential to pay particular attention to future developments in this area.

111. **Therefore, the EDPB invites the European Commission to observe any developments with regard to the allocation of resources to the ICO, which would be detrimental to the proper fulfilment of the ICO's tasks.**

3.2.2. Existence of a data protection system ensuring a good level of compliance

112. The draft decision undertakes a comprehensive examination of the powers that the ICO is equipped with under Article 58 UK GDPR and the DPA 2018 in order to ensure the monitoring and enforcement of the legislation. The EDPB acknowledges that Article 58 UK GDPR mirrors in a close manner the corresponding rules with regard to powers of SAs as set forth in Article 58 GDPR. Regarding the power to impose administrative fines depending on the circumstances of each individual case, Article 83 UK GDPR contains similar provisions and maximum amounts as set forth in Article 83 GDPR. Hence, the EDPB considers the UK legal framework in this field currently to be in line with the standards as set forth in the relevant law of the EU. In that respect, the EDPB nevertheless highlights that the existence of *effective* sanctions plays an important role in ensuring respect for rules.[73]

113. **In the light of the above, the EDPB invites the European Commission to monitor the effectiveness of sanctions and relevant remedies in the UK Data Protection Framework.**

3.2.3. The data protection system must provide support and help to data subjects in the exercise of their rights and appropriate redress mechanisms

114. An effective supervision mechanism, allowing independent investigation of complaints so as to identify and punish infringements of data subject rights in practice, as well as an effective administrative and judicial redress (including compensation for damages as a result of the unlawful processing of data subject's personal data), are key elements for the assessment of whether a data protection system provides an adequate level of protection.

115. The EDPB welcomes that the ICO provides comprehensive information and guidelines on its website, which aim to raise awareness among controllers and processors in relation to their obligations and duties, as well as to support data subjects in order to be informed about their personal data rights and to assert their individual rights under the UK GDPR and the DPA 2018.

116. **Notwithstanding the current state, the EDPB invites the European Commission to continuously observe the level of support the ICO provides specifically to individuals, whose personal data have been transferred to the UK under the adequacy decision, to help them exercise their rights under the UK data protection regime.**

[72] European Parliament resolution of 25 March 2021 on the Commission evaluation report on the implementation of the General Data Protection Regulation two years after its application, para. 15, https://www.europarl.europa.eu/doceo/document/B-9-2021-0211_EN.html.
[73] See WP 254 rev.01, p. 7.

4. ACCESS AND USE OF PERSONAL DATA TRANSFERRED FROM THE EU BY PUBLIC AUTHORITIES IN THE UK

4.1. Access and use by UK public authorities for criminal law enforcement purposes

4.1.1. Legal bases and applicable limitations/safeguards

117. Regarding the assessment performed by the European Commission and documented in recitals 132 and following of the draft decision **on access for law enforcement purposes**, the European Commission provides nuanced and detailed information, and generally reaches comprehensible conclusions. Therefore, the EDPB refrains from reproducing most of the factual finding and assessments in this opinion. There are, however, certain instances where the depiction of the facts or the explanation of the conclusions do not suffice in order for the EDPB to espouse them.

4.1.1.1. The use of consent

118. The EDPB takes note that the European Commission asserts in footnote 184 of the draft decision[74] that **the use of consent** is not relevant in an adequacy scenario, as in transfer situations the data are not directly collected from a data subject by a UK law enforcement authority on the basis of consent. Consequently, the use of consent as a legal basis in policing is not assessed by the European Commission.

119. In this regard, the EDPB recalls that Article 45(2)(a) GDPR requires assessing a broad array of elements not limited to the transfer situation, including "*the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including [...] criminal law*".

120. The EDPB notes, based also on the information provided by the European Commission in recital 38 of its draft implementing decision pursuant to Directive (EU) 2016/680 of the European Parliament and of the Council on the adequate protection of personal data by the UK (hereinafter "draft LED adequacy decision"), that the use of consent, as framed in the UK regime in the context of law enforcement, would always require a legal basis to be relied upon. This means that even if the police have statutory powers to process the data for the purpose of an investigation, in certain specific circumstances (for example to collect a DNA sample), the police may consider appropriate to ask for the consent of the data subject.

121. **The EDPB invites the European Commission to introduce in the adequacy decision its analysis on the possible use of consent in a law enforcement context, provided for in the draft LED adequacy decision**.

4.1.1.2. Search warrants and production orders

122. While the EDPB has no comments on the retrieval of evidence by the police through search warrants and production orders in general, it stems from recital 136 of the draft decision that the European Commission has centred its law enforcement access considerations around the police, and that the processing of personal data by other law enforcement agencies was less examined.

[74] See p. 37 of the draft decision.

123. For example, the UK Explanatory Framework for Adequacy Discussions, Section F: Law Enforcement[75], suggests on p.11 that **the National Crime Agency** (hereinafter "NCA") could be a law enforcement agency of particular interest, which *inter alia* has a wider criminal intelligence function. The NCA describes its mission as bringing together intelligence from a range of sources in order to maximise analysis, assessment and tactical opportunities, including from technical interception of communications, law enforcement partners in the UK and overseas, security and intelligence agencies[76]. The NCA is also one of the main interlocutors for the international law enforcement partners, and plays a key role in the exchange of criminal intelligence[77].

124. The EDPB further takes note of the fact that the Government Communications Headquarters (hereinafter "GCHQ"), whose activities typically fall under the scope of Part 4 DPA 2018, i.e. national security, assumes as well an active role in reducing the societal and financial harm which serious and organised crime causes to the UK, working closely with the Home Office, NCA, HM Revenue and Customs ("HMRC"), and other government departments[78]. Its activities relate to countering child sexual abuse; fraud; other types of economic crime, including money laundering; criminal use of technology; cybercrime; organised immigration crime, including people trafficking; and drugs, firearms and other illicit smuggling activity.

125. **The EDPB calls on the European Commission to complement its analysis with an analysis of the agencies active in the field of law enforcement that seem to have made collecting and analysing data, including personal data, a focus of their day-to-day operations, in particular the NCA. In addition, the EDPB invites the European Commission to have a closer look into the agencies like the GCHQ, whose activities fall both within the scope of law enforcement and national security, and the legal framework applicable to them for the processing of personal data.**

4.1.1.3. Investigatory powers for law enforcement purposes

126. Under Chapter 4 the GDPR Adequacy Referential 'Essential guarantees in third **countries for law enforcement** and national security access to limit interferences to fundamental rights', the EDPB recalls that *"[i]n this context, the court also noted critically that the previous Safe Harbor decision did*

[75] See UK Government, Explanatory Framework for Adequacy Discussions, Section F: Law Enforcement, 13 March 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872237/F_-_Law_Enforcement_.pdf.

[76] See National Crime Agency's website, Intelligence: enhancing the picture of serious organised crime affecting the UK, https://www.nationalcrimeagency.gov.uk/what-we-do/how-we-work/intelligence-enhancing-the-picture-of-serious-organised-crime-affecting-the-uk.

[77] While not all intelligence processed by the NCA is personal data, a substantial portion might be personal information and the activities here described differ from those of classic policing, so that an assessment of access to personal data by law enforcement in the UK would be incomplete without thoroughly assessing the activities of the NCA. It seems reasonable to make sure that data protection principles are awarded the same meaning across all relevant law enforcement agencies, therefore shedding light on an especially data-driven agency such as the NCA. In addition, in "looking to the future", the explanation continues, *"[w]e continuously look for new opportunities to collect, develop and enhance traditional capabilities to increase the quantity and quality of intelligence available to exploit both in the UK and abroad." "As part of this we are developing the new National Data Exploitation Capability, using the powers vested in the agency by the Crime and Courts Act, to link together, access and exploit data held across government."* [...] *"All of this will increase our agility and flexibility to respond to new threats and operate in a proactive way, to gather and analyse information and intelligence on emerging threats so that we can take action before threats are realised."*

[78] See GCHQ's website, Mission, Serious and Organised Crime, https://www.gchq.gov.uk/section/mission/serious-crime.

*"not contain any finding regarding the existence, in the United States, of rules adopted by the State intended to limit any interference with the fundamental rights of the persons whose data is transferred from the European Union to the United States, **interference which the State entities of that country would be authorized to engage in when they pursue legitimate objectives**, such as national security.""*[79]. In this Referential, the EDPB states that the **four European Essential guarantees**[80] **need to be respected for access to data, whether for** national security purposes or **for law enforcement purposes, by all third countries in order to be considered adequate,** in particular **the necessity and proportionality with regard to legitimate objectives pursued need to be demonstrated.**

127. Under this section of the draft decision, the European Commission concludes (recital 139) *"since investigatory powers provided by the IPA 2016 are the same as those available to national security agencies, the conditions, limitations and safeguards applicable to such powers are addressed in detail in the Section on access and use of personal data by UK public authorities for national security purposes*". However it stems from the case-law of the CJEU, when applying the necessity and proportionality test to Member States' legislation allowing for retention and access to personal data by public authorities, that legitimate objectives, such as national security or fighting serious crimes, are different and, therefore, one might be able to justify a certain type of interference while the other might not[81].

128. **The EDPB would therefore welcome a specific assessment within the decision of the necessity and proportionality of the conditions, limitations and safeguards described under recitals 174 and following - which is a section devoted to measures pursuing national security objectives - when it comes to applying these conditions, limitations and safeguards in the context of a measure pursuing a law enforcement objective. It thus invites the European Commission to further clarify whether the described retention of personal data and access to it for law enforcement purposes are sufficiently limited, so as to ensure an essentially equivalent level of protection to that guaranteed within the EU.**

4.1.2. Further use of the information collected for law enforcement purposes (recitals 140-154)

129. The EDPB notes that the UK Data Protection Framework provides for similar safeguards and limitations than the ones provided under EU law in relation to the further use of the information collected for law enforcement purposes.

4.1.2.1. Further use for other law enforcement purposes

130. The DPA 2018 indeed provides that personal data collected by a competent authority for a law enforcement purpose may be further processed (whether by the original controller or by another controller) for any other law enforcement purpose, provided that the controller is authorised by law to process data for the other purpose, and the processing is necessary and proportionate to that purpose. The European Commission notes that all the safeguards provided by Part 3 DPA 2018 apply to the processing carried out by the receiving authority. The EDPB highlights however that, under Part 3 DPA 2018, sections 44(4), 45(4), 48(3) and 68(7) provide for the possibility to restrict the rights of data subject, and section 79 provides for the possibility of issuing certificates attesting that a restriction is a necessary and proportionate measure to protect national security. **The EDPB therefore recommends that the European Commission further assess the possible impact of such restrictions to the level of protection of personal data in relation to the further use of the information collected. Similarly, further clarification should also be provided in relation to the UK legal framework allowing for such onward sharing, in particular the Digital Economy Act 2017, as well as the Crime and Courts Act 2013 that allows for the sharing of information with the NCA.**

[79] See WP254 rev.01, p.9.
[80] See EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures.
[81] See CJEU, joined cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and others*, 6 October 2020, ECLI:EU:C:2020:791.

4.1.2.2. Further use for other purposes than law enforcement within the UK

131. The DPA 2018 also provides that personal data collected for any law enforcement purpose may be processed for a purpose that is not a law enforcement one when the processing is authorised by law. In this case, the legal basis authorising such sharing is section 19 Counter-Terrorism Act 2008. In this regard, the EDPB notes that the scope and provisions of section 19 Counter-Terrorism Act is not fully addressed in the European Commission's assessment, and may imply further use of a broader nature, in particular as regards section 19(2) which provides that "*[i]nformation obtained by any of the intelligence services in connection with the exercise of any of its functions may be used by that service in connection with the exercise of any of its other functions*."

132. The EDPB also notes that the European Commission's reference to the fact that competent authorities are public authorities that must act in compliance with ECHR, including Article 8 thereof, thus ensuring that all data sharing between the law enforcement agencies and the intelligence services complies with data protection legislation, and with the ECHR, could be further substantiated by identifying the relevant acts and laws under the UK legal order laying down clearly and precisely such limits.

4.1.2.3. Further use in the context of onward transfers outside the UK

133. While the European Commission has referred to the fact that the UK-US CLOUD Act Agreement may affect onward transfers to the US from CSPs in the UK, the EDPB also highlights that the entry into force of this agreement may also affect the further use of the information collected through onward transfers from law enforcement authorities in the UK, in particular in relation to the issuance and transmission of orders as per Article 5 UK-US CLOUD Act Agreement.

134. More broadly, the EDPB considers that the conclusion of future bilateral agreements with third countries for the purpose of law enforcement cooperation, providing a legal basis for the transfer of personal data to these countries, may also significantly affect the conditions for further use of the information collected, since such agreements may affect the UK Data Protection Framework as assessed. The EDPB therefore recommends that the European Commission further assess this point, identifying the existence of international agreements, and clarifies whether the provisions of these agreements may affect the application of UK data protection law and provide for further limitation or exemption in relation to the further use and disclosure overseas of information collected for law enforcement purposes. The EDPB considers that such information and assessment are essential in order to allow a comprehensive assessment of the level of protection afforded by the UK legislative framework and practices in relation to overseas disclosure and further use.

4.1.3. Oversight

135. The EDPB notes that the oversight of criminal law enforcement agencies is ensured by a combination of different Commissioners, in addition to the ICO. The draft adequacy findings mention the IPC, the Commissioner for the Retention and Use of Biometric Material, as well as the Surveillance Camera Commissioner. In this context, it is to be noted that the CJEU has repeatedly stressed the need for independent oversight. Of particular importance on questions of access to personal data transferred

to the UK is the IPC. The understanding of the EDPB is that the IPC is a so-called "judicial commissioner", as other judicial commissioners, to be referred to in the context of the national security chapter, and that those judicial commissioners enjoy the independence of judges, also when serving as commissioners. As to the office of the IPC, the European Commission explains in recital 245 of the draft decision that it functions independently as a so-called "arm's length body", while being funded by the Home Office.

136. The EDPB has not found in the draft decision further indication to assess the independence of the Commissioner for the Retention and Use of Biometric Material, as well as of the Surveillance Camera Commissioner.

137. **The European Commission is invited to further assess the independence of the judicial commissioners, also in cases where the Commissioner is not (anymore) serving as a judge, as well as to assess the independence of the Commissioner for the Retention and Use of Biometric Material, and of the Surveillance Camera Commissioner.**

4.2. General legal framework on data protection in the field of national security

4.2.1. National security certificates

138. According to section 111 DPA 2018, controllers may apply for national security certificates issued by a Minister, member of the Cabinet, the Attorney general or the Advocate General for Scotland, certifying that exemptions from obligations and rights enshrined in Parts 4 to 6 DPA 2018 are a necessary and proportionate measure for the protection of national security. These certificates are meant to give controllers greater legal certainty, and will be conclusive evidence of the fact that national security is applicable when processing personal data. However, it should be mentioned that these certificates are not required in order to rely on national security exemptions, but instead are a measure of transparency[82].

139. The EPDB understands from Schedule 20 DPA 2018, sections 17 and 18 that a national security certificate issued under the Data Protection Act 1998 (hereinafter "old certificate") had an extended effect for the processing of personal data under the DPA 2018 until 25 May 2019. Until this date, unless replaced or revoked, the old certificates were treated as if they were issued under the DPA 2018.

140. However, where there is no express expiry date on a national security certificate issued under the Data Protection Act 1998, the EDPB understands that such a certificate will continue to have effect in relation to processing under the Data Protection Act 1998, unless the certificate is revoked or quashed[83]. Even though the protection provided by these old certificates is limited to the processing of personal data under the Data Protection Act 1998, the EDPB takes note that new national security certificates can be issued under the Data Protection Act 1998 for personal data that was processed under the Data Protection Act 1998.[84]

[82] See Home Office, The Data Protection Act 2018, National Security Certificates guidance, August 2020, para 4, p. 3, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf.
[83] See Home Office, The Data Protection Act 2018, National Security Certificates guidance, August 2020, p. 5.
[84] See Home Office, The Data Protection Act 2018, National Security Certificates guidance, August 2020, para 8, p. 5.

141. **For the sake of comprehensiveness, the EDPB invites the European Commission to clarify in its draft decision that national security certificates can still be issued under the Data Protection Act 1998. Moreover, the EDPB invites the European Commission to describe in its draft decision the redress and oversight mechanisms with regard to certificates issued under the Data Protection Act 1998. Finally, the EDPB invites the European Commission to include in its draft decision the number of existing certificates issued under the Data Protection Act 1998, and to attentively monitor this aspect.**

4.2.2. Right to rectification and erasure

142. With regard to the right to rectification and erasure, the EDPB takes note that, in accordance with section 100 and section 149 DPA 2018, data subjects have the possibility to rely on the High Court (in Scotland, the Court of Session) to order a controller to rectify or delete their data without undue delay.

143. **The EDPB stresses that the exercise of data subjects' rights needs to be effectively ensured; therefore invites the European Commission to describe in its draft decision how section 100 DPA 2018 works in practice, and to closely monitor the application of this section.**

4.2.3. Exemptions for National Security

144. The EDPB wants to draw attention to section 110 DPA 2018, and in particular to Schedule 11, which sets out the specific purposes for which intelligence services can deviate from certain data protection principles, including in relation to data subjects' rights, and are not obliged to communicate personal data breaches to the ICO.[85]

145. The **EDPB calls the European Commission to clarify further the scope of the exemptions as it wonders whether all of the exemptions provided under Schedule 11 DPA 2018 are relevant for the work of intelligence services, and whether they ensure the equivalence with the necessity and proportionality principle**. In particular, **the EDPB invites the European Commission to provide more clarification under which circumstances an intelligence service could rely on section 10 of Schedule 11 DPA 2018, which states that "*[t]he listed provisions do not apply to personal data that consists of records of the intentions of the controller in relation to any negotiations with the data subject to the extent that the application of the listed provisions would be likely to prejudice the negotiations.*"**

4.3. Access and use by UK public authorities for national security purposes

146. As a general remark, the EDPB acknowledges that States are granted a broad margin of appreciation in matters of national security, which is also recognised by the ECtHR. The EDPB also recalls that, as underlined in its updated recommendations on the European essential guarantees for surveillances measures[86], Article 6(3) Treaty on European Union establishes that the fundamental rights enshrined in the ECHR constitute general principles of EU law. However, as the CJEU recalls in its jurisprudence,

[85] These purposes are the prevention and detection of "Crime", "Information required to be disclosed by law etc or in connection with legal proceedings", "Parliamentary privilege", "Judicial proceedings", "Crown honours and dignities", "Armed forces", "Economic well-being", "Legal professional privilege", "Negotiations", "Confidential references given by the controller", "Exam scripts and marks", "Research and statistics" and "Archiving in the public interest".
[86] See EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures.

the latter does not constitute, as long as the EU has not acceded to it, a legal instrument which has been formally incorporated into EU law[87]. Thus, the level of protection of fundamental rights required by Article 45 GDPR must be determined on the basis of the provisions of that regulation, read in the light of the fundamental rights enshrined in the EU Charter. This being said, according to Article 52(3) EU Charter, the rights contained therein that correspond to rights guaranteed by the ECHR are to have the same meaning and scope as those laid down by the ECHR. Consequently, as recalled by the CJEU, the jurisprudence of the ECtHR concerning rights that are also foreseen in the EU Charter must be taken into account, as a minimum threshold of protection to interpret corresponding rights in the EU Charter[88]. According to the last sentence of Article 52(3) EU Charter, however, *"[t]his provision shall not prevent Union law providing more extensive protection."*

147. Therefore, in the following assessment, the EDPB has taken into account the jurisprudence of the ECtHR, to the extent that the EU Charter, as interpreted by the CJEU, does not provide for a higher level of protection which prescribes other requirements than the ECtHR case-law.

4.3.1. Legal bases, limitations and safeguards - Investigatory powers exercised in the context of national security

4.3.1.1. General remarks

148. The EDPB recalls that the IPA 2016 is a recent law that amended several provisions of the Intelligence Services Act 1994. It sets out the extent to which certain investigatory powers may be used to interfere with privacy[89]. Despite two reports of the IPC that provide useful information concerning the application of this new legal framework, there is still no review of certain aspects, in particular concerning the selectors and search criteria used.

149. Also, as a general remark concerning the IPA 2016 and its scope of application, the EDPB highlights the following four points of attention:

150. In relation to the **first point of attention**, with regard to the features of the law, the EDPB would like to underline two aspects:

151. First, the EDPB notes that the legislation refers to broad purposes for the use of procedures provided for in the IPA 2016 and not to the categories of individuals who may be concerned by the collection of data on the basis of Parts 2 to 7 IPA 2016. In this regard, the EDPB recalls that there should be a link between the categories of individuals who may be the subject of surveillance measures and the purposes pursued by the legislation to define the personal scope of the law.

152. Furthermore, the EDPB also stresses that the definition of "telecommunications operators", "telecommunications service" and "telecommunications system", which define the scope of the law, are also very broad and unclear to some extent. Indeed, the EDPB highlights that these notions, in the field of the IPA 2016, have to be understood in a much broader manner than under the telecommunications legislations, as defined for instance in the European Electronic Communications Code[90]. The EDPB notes that the definitions of "telecommunications service" and

[87] See *Schrems II*, para. 98.
[88] See CJEU, joined cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and others*, 6 October 2020, ECLI:EU:C:2020:791, para. 124.
[89] See section 1 IPA 2016.
[90] See Article 2 (5) of the European Electronic Communications Code which defines, for instance, 'interpersonal communications service' as *"a service normally provided for remuneration that enables direct interpersonal and interactive exchange of information via electronic communications networks between a finite number of persons, whereby the persons initiating or participating in the communication determine its recipient(s) and does not include services which enable interpersonal and interactive communication merely as a minor ancillary feature that is intrinsically linked to another service"*.

"telecommunication system" in the Act are said to be intentionally broad so that they will remain relevant for new technologies. Likewise, the definition of a telecommunications operator is also very broad, and could for instance include online videogames with a chat feature included, or other online websites merely including such chat windows[91].

153. In addition, whereas procedures and oversight concerning the assessment of the necessity and proportionality of collection and access to data are generally provided, the criteria to proceed to such an assessment are not defined in the law itself. Additional elements can be found in other documents, such as Codes of practice.

154. However, as recalled in the EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, the CJEU has indicated that *"the requirement that any limitation on the exercise of fundamental rights must be provided for by law implies that the legal basis which permits the interference with those rights must itself define the scope of the limitation on the exercise of the right concerned"*[92]. More precisely, the CJEU clarified that *"[i]n order to satisfy the requirement of proportionality, the legislation must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, so that the persons whose personal data is affected have sufficient guarantees that data will be effectively protected against the risk of abuse. That legislation must be legally binding under domestic law and, in particular, must indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary."*[93]

155. The ECtHR also stressed the importance of the clarity of the law to give individuals *"an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures"*[94].

156. **The EDPB therefore calls on the European Commission to further assess these aspects concerning the preciseness, clarity and exhaustiveness of the relevant law, and to provide further elements to demonstrate it provides a level of protection essentially equivalent to that guaranteed within the EU with regard to the features of the law. The EDPB also stresses that broad definitions should also be assessed in relation to the proportionality of the interception measures.**

157. In addition, although several internal codes of the competent intelligence community authorities partly develop some of these elements, for instance concerning the assessment of the necessity and proportionality of collection of data, the EDPB stresses that the requirements of the CJEU in relation to the nature of the law imply that the core elements, including for individuals to be able to rely on

[91] See Home Office, Code of practice on the interception of communications, March 2018, paras 2.5 and following, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf.
[92] See *Schrems II*, para. 175; and the case-law cited, as well as CJEU, case C-623/17, *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs and Others*, 6 October 2020, ECLI:EU:C:2020:790 (hereinafter "Privacy International"), para. 65.
[93] See *Privacy International*, para. 68.
[94] See ECtHR, *Zakharov v. Russia*, 4 December 2015, CE:ECHR:2015:1204JUD004714306, para. 229.

them in the context of redress, must be provided in legislation providing for actionable rights[95]. Indeed, Schedule 7, paragraph 6 IPA 2016 mentions the fact that courts (and supervisory authorities) "*take into account a failure by a person to have regard to a code in determining a question in any such proceedings*" without clarifying whether individuals can claim a breach of the codes before courts (or supervisory authorities). Moreover, the elements provided so far in the draft decision either refer to the recognition by the ECtHR of the foreseeability of the rules provided[96] in those codes, rather than to their "actionability" in court, as required by the CJEU, or to the fact that UK Courts have in some cases referred to codes, while none of the cases mentioned illustrate the possibility for individuals to action rights derived from the codes. **If it is concluded that UK law does not indicate sufficiently the circumstances and conditions under which a measure may be adopted and that these elements are in fact provided by internal codes of the intelligence community authorities, the EDPB would thus call on the European Commission to further assess whether the limitations and safeguards provided in the different internal codes of the intelligence community authorities may be actioned by individuals before a court and enforced.**

158. **The second point of attention** concerns the fact that the provisions relating to, on the one hand, targeted acquisition and retention of communications data and, on the other hand, to bulk collection, either in the IPA 2016 or in other legislations such as the Intelligence Services Act 1994, or the Regulation of Investigatory Powers Act 2000, will also apply to data transferred from the EU to the UK. Concerning bulk collection, the EDPB underlines that the relevant provisions of UK law allow for the collection of data outside the UK; thus could include data in transit transferred from the EEA to the UK on the basis of the adequacy decision[97]. Moreover, the EDPB notices that the European Commission indicates that "*[i]t should be noted that the retention and acquisition of communications data normally does not concern personal data of EU data subjects transferred under this Decision to the UK. The obligation to retain or disclose communications data pursuant to Part 3 and 4 of the IPA 2016 covers data that is collected by telecommunication operators in the UK directly from the users of a telecommunication service.*"[98] Nevertheless, the EDPB highlights the lack of clarity concerning the fact that only establishments of these operators situated in the UK can receive requests from the competent UK authorities since the definition of telecommunications operator provided in section 261(10) IPA 2016 requires that "a telecommunications operator is a person who offers or provides a telecommunications service to persons in the UK *or who controls or provides a telecommunication system which is (wholly or partly) in or controlled from the UK*". Consequently, personal data of EEA data subjects could actually be concerned, for instance in the case of data collected or generated by an establishment of a UK telecommunications operator located within the EEA, transferred to an establishment of this same operator situated in the UK on the basis of the adequacy decision (for commercial purposes), and then collected, within the UK, by the competent public authorities.

[95] In this regard, the CJEU considered for instance that PPD 28 in the US, did not qualify, although it provided also some limitations with regard to bulk collection, see *Schrems II*, para 181.
[96] See ECtHR, *Big Brother Watch and others v. the United Kingdom*, 13 September 2018, ECLI:CE:ECHR:2018:0913JUD005817013 (hereinafter "Big Brother Watch"), para. 325: "*As the IC Code is a public document, subject to the approval of both Houses of Parliament, and has to be taken into account both by those exercising interception duties and by courts and tribunals, the Court has expressly accepted that its provisions could be taken into consideration in assessing the foreseeability of the RIPA regime.*"
[97] See para 183 and following of *Schrems II* on the assessment of a legislation providing for access to data in transit between the EU and a third country in the context of an adequacy decision.
[98] See recital 196 of the draft decision.

159. **The EDPB is therefore of the view that the assessment of these provisions are also relevant for the assessment of the level of adequacy of the UK legal framework and calls on the European Commission to clarify this aspect, and further assess to what extent this is the case. In particular, the EDPB calls on the European Commission to clarify its understanding of the scope of this legislation, including of what the notion of "users of telecommunications services" covers, and whether data from establishments of telecommunications operators outside the UK, to the extent that data of EEA data subjects are concerned, could be requested, given the very broad definition of telecommunications operators.**

160. **The third point of attention** concerns the "double-lock" procedure. The EDPB notes that a new "double-lock" procedure has been introduced in the IPA 2016. Nonetheless, the EDPB also understands that even if, in principle, collection or access to data for national security or intelligence purposes can only take place with a warrant approved by a Judicial Commissioner, the IPA 2016 provides that "*in specific limited cases lawful interception without a warrant is possible and only prior authorisation by the competent IC authorities themselves is required [see infra section on Oversight], including for interceptions in accordance with overseas requests (section 52 of the IPA 2016)*". As underlined hereafter, this also concurs to the concerns of the EDPB with regard, notably, to overseas disclosures. In addition, the EDPB also notes that for equipment interference, be it targeted or in bulk, a derogation to the double-lock procedure is also possible, and that the Judicial Commissioner is entitled to approve only the renewal of bulk warrants, after a maximum initial period of 6 months. **The EDPB calls on the European Commission to further assess and demonstrate that even in cases where the double-lock procedure does not apply, the UK legal framework provides for appropriate safeguards, including through the effective *ex post* oversight and redress possibilities offered to the individuals, to ensure that the level of protection provided is essentially equivalent to the one provided within the EU (see also infra section 4.3.3 on Oversight).**

161. Moreover, although the IPA 2016 has indeed introduced the "double-lock" procedure, the EDPB remains concerned with regard to certain features of the new legislation. Following the presentation of the corresponding sections of the draft decision, the EDPB has analysed the following types of collection and access to data in the same order as presented by the European Commission. The order of the elements assessed hereafter therefore does not reflect a hierarchy in terms of level of concern of the EDPB.

4.3.1.2. Targeted acquisition and retention of communications data

162. The EDPB notes that there are two officials who can grant targeted authorisations for obtaining communications data: the authorising officer in the Office for Communications Data Authorisations (hereinafter "the IPC"), a designated senior officer (a person holding a prescribed office or rank in a relevant public authority), in addition to the approval by a Judicial Commissioner in certain cases. However, it remains unclear for the EDPB, under the law and the relevant code, exactly which official authorises which type of targeted acquisition of communications data, and to what extent a designated officer would be sufficiently independent[99].

163. **The EDPB consequently calls on the European Commission to further assess this aspect and provide clearer explanations on these elements.**

164. Concerning the notice requiring the retention of communication data, the EDPB also notes that such notices can be addressed to a "description of operators". This notion appears to mean that several

[99] See also infra concerning the assessment of the double-lock procedure and the independence of the Judicial Commissioner.

operators can be requested at the same time to all retain data. Indeed, the targeted nature of the acquisition does not relate to the number of operators, but to the name or description of persons, organisations, location or group of persons that constitute the "target", a description of the nature of the investigation and a description of the activities for which the equipment is used. The EDPB therefore highlights that, depending on the number of operators concerned by such "description of operators", the notice may be broader than what the procedure for targeted retention may seem to imply. **The EDPB invites the European Commission to further assess this aspect, and to provide further assurances that, even when notices are addressed to several operators, they remain limited to what is strictly necessary and proportionate.**

4.3.1.3. Equipment interference

165. The EDPB notes that "equipment interference" can derogate from the double-lock procedure in case of urgency[100]. The EDPB is therefore concerned that the purposes for which such equipment interference can be required are broad, and that the criteria for urgency (in which case the Judicial Commissioner is not required to provide an *ex ante* authorisation following an assessment of the necessity and proportionality of the equipment interference) remain unclear. Since in the latter situation "the warrant ceases to have affect and may not be renewed" in case where the Judicial Commissioner does not approve the equipment interference *ex post*, the EDPB understands that the data collected meanwhile remain lawfully collected. For these data to be deleted, a specific order of the Judicial Commissioner may be issued[101].

166. **The EDPB calls on the European Commission to further assess the conditions under which urgency can be invoked, and to provide clarifications concerning the possible avenues for the exercise of rights for the data subjects concerned, and possible redress avenues offered to them in the context of equipment interference operations, especially when they take place in the context of urgency leading to a derogation to the double-lock procedure.**

4.3.1.4. Bulk interception of data from bearers

167. As described in the report of the bulk powers review[102] "*[b]ulk interception typically involves the collecting of communications as they transit particular bearers (communication links)*." The official IPA 2016 factsheet describes "bulk interception" as "*the process for the collection of a volume of communications followed by the selection of specific communications to be read, looked at or listened to where it is necessary and proportionate*." The EDPB notes that "bulk interception" of data actually implies the collection of data even before any filtering by selectors (either simple in the context of the monitoring of individuals already known to pose a threat, or complex, in the context of the identification of new threats and of previously unknown persons of interest).

168. The acquisition of bulk communications data was also one of the issues examined by the CJEU in the Privacy International case, which resulted in a judgment of the Grand Chamber issued on 6 October 2020 (in addition to whether such collection of data was performed in the context of EU law, even for national security purposes). The IPA 2016 has replaced the legislation that was the subject of this judgment.

169. The EDPB notes that, with the introduction of the IPA 2016 in UK law, a warrant is now required also to intercept data in bulk. The process to issue this warrant relies on the determination of "operational purposes". The list of these operational purposes is established by heads of intelligence services, and

[100] See section 109 IPA 2016.
[101] See section 110, subsection 3, point b) IPA 2016.
[102] See Report of the bulk powers review, by the Independent Reviewer of Terrorism Legislation, August 2016.

then approved by the Secretary of State. This decision is itself approved by an independent Judicial Commissioner who must review whether the warrant is necessary and proportionate to the operational purposes. The EDPB understands that the Judicial Commissioner does not have the power to assess the operational purposes themselves, but whether the warrant is necessary and proportionate to the operational purposes listed in the warrant. The Parliamentary Intelligence and Security Committee is provided with a copy of the list every three months, and the Prime Minister reviews the list of these operational purposes at least once a year.

170. However, on the basis of the elements provided by the European Commission in the draft decision, it appears difficult to assess the scope of these operational purposes provided in the list and whether the collection of data they allow meets the threshold set by the CJEU (for instance circumscribing the collection of data to a geographical area could be as narrow as a few streets, as well as collecting data from the EEA as a whole).

171. In addition, the EDPB underlines that data collected in bulk may be retained for long periods (to be available for further access for examination). Indeed, the EDPB notes that section 150, paragraphs 5 and 6 IPA 2016 provide only for the destruction of the copies of the data collected, and only if their retention is not necessary, or not likely to become necessary, in the interests of national security or any other grounds falling under the scope of section 138(2) IPA 2016, or if the retention is not necessary for several other purposes[103]. The EDPB stresses that these grounds appear very broad, and in any case only copies of the data obtained are mentioned.

172. Furthermore, the EDPB also notes that in urgent cases, the IPA 2016 also allows for the modification of warrants without the prior-approval of a Judicial Commissioner, and that in such case, if the Judicial Commissioner consulted *ex post* within three working days after the modification refuses to approve the modification, the warrant should have effect as if the modification had not been made, but the data collected in-between remain collected lawfully[104]. For these data to be deleted, a specific order of the Judicial Commissioner may be issued[105].

173. **The EDPB therefore calls on the European Commission for further clarifications and assessment of bulk interceptions, in particular on the selection and application of selectors in the context of these bulk interception procedures to clarify the extent to which access to personal data meets the threshold set by the CJEU (see also below section 4.3.1.7., in particular on the oversight on the selectors), and which safeguards are in place to protect the fundamental rights of individuals whose data are intercepted in this context, including concerning the retention periods of data. An independent assessment from UK competent oversight authorities would be particularly useful.**

174. **The EDPB also underlines that it seems all the more critical that "overseas-related communications" which are within the scope of bulk interception practices appear to imply that data could be directly intercepted and collected in bulk within the EEA by the UK, including for data in transit between the EEA and the UK that would fall within the scope of the draft decision (see below section 4.3.2. on further use of the information collected for national security purposes and overseas disclosure).**

[103] See subsections 3 and 6 of section 150 IPA 2016.
[104] See section 147 IPA 2016 (Part 6, chapter I).
[105] See section 181, subsection 3, point b) IPA 2016.

4.3.1.5. Protection and safeguards for secondary data

175. In addition, the EDPB is concerned that the UK relevant legislation related to bulk interception does not provide for the same level of protection to all communications data. "Secondary data", which can be obtained with a bulk warrant are, according to section 137 IPA 2016, both "systems data", "*which is comprised in, included as part of, attached to or logically associated with the communication (whether by the sender or otherwise)*", and "identifying data", "*which is comprised in, included as part of, attached to or logically associated with the communication (whether by the sender or otherwise), is capable of being logically separated from the remainder of the communication, and if it were so separated, would not reveal anything of what might reasonably be considered to be the meaning (if any) of the communication, disregarding any meaning arising from the fact of the communication or from any data relating to the transmission of the communication*"[106].

176. The EDPB notes that these "secondary data", also known as "metadata"[107], collected in bulk, seem not to benefit from the same safeguards as data collected with a targeted warrant, but also as content data collected in bulk. Indeed, the EDPB notices that the selection of any of the intercepted content benefits from more safeguards[108] than the selection of secondary data[109].

177. Furthermore, the EDPB stresses that both the ECtHR[110] and the CJEU[111] have questioned the fact that such data are less sensitive than others, and in particular than content data. Indeed, the Code of Practice concerning interceptions presents as examples of "secondary data" (both "systems data" such as router configurations, email addresses or users ID; but also alternative account identifiers, as well as "identifying data", such as the location of a meeting in a calendar appointment, photograph information, such as the time, date and location when it was taken). **The EDPB thus stresses the consistent assessment by the ECtHR and the CJEU, and recalls the concerns expressed in relation to secondary data that should benefit from specific safeguards due to their sensitivity. The EDPB therefore calls on the European Commission to carefully assess whether the safeguards provided under UK law for such category of personal data ensure an essentially equivalent level of protection to the one guaranteed in the EU.**

[106] "Systems data" and "identifying data" are defined in section 263 IPA 2016.
[107] See Report of the bulk powers review, by the Independent Reviewer of Terrorism Legislation, August 2016.

[108] See section 152, subsection 1, point c) and subsections 3 and following IPA 2016.
[109] See section 152, subsection 1, points a) and b) IPA 2016.
[110] See ECtHR, *Big Brother Watch*, para. 357, under referral to the Grand Chamber: "*Consequently, while the Court does not doubt that related communications data is an essential tool for the intelligence services in the fight against terrorism and serious crime, it does not consider that the authorities have struck a fair balance between the competing public and private interests by exempting it in its entirety from the safeguards applicable to the searching and examining of content. While the Court does not suggest that related communications data should only be accessible for the purposes of determining whether or not an individual is in the British Islands, since to do so would be to require the application of stricter standards to related communications data than apply to content, there should nevertheless be sufficient safeguards in place to ensure that the exemption of related communications data from the requirements of section 16 of RIPA is limited to the extent necessary to determine whether an individual is, for the time being, in the British Islands..*"
[111] See CJEU, *Privacy International*, para. 71: "*The interference with the right enshrined in Article 7 of the Charter entailed by the transmission of traffic data and location data to the security and intelligence agencies must be regarded as being particularly serious, bearing in mind inter alia the sensitive nature of the information which that data may provide and, in particular, the possibility of establishing a profile of the persons concerned on the basis of that data, such information being no less sensitive than the actual content of communications. In addition, it is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance (see, by analogy, judgments of 8 April 2014, Digital Rights Ireland and Others, C-293/12 and C-594/12, EU:C:2014:238, paragraphs 27 and 37, and of 21 December 2016, Tele2, C-203/15 and C-698/15, EU:C:2016:970, paragraphs 99 and 100).*"

4.3.1.6. Automated processing of communications data

178. The EDPB notes that intelligence community authorities do not only use simple or complex selectors to filter the data acquired in bulk, but that they may also rely on other automated processing tools to analyse "*large volumes of information, which enables the Agencies also to find linkages, patterns, associations or behaviours which might demonstrate a serious threat requiring investigation*", according to the Intelligence and Security Committee report 2015[112]. **The EDPB is aware of the fact that this public report concerns practices under the previous legal framework, which was subsequently replaced by the IPA 2016. Nevertheless, it sees a need for further independent assessment and oversight of the use of automated processing tools by the competent UK oversight authorities, and calls on the European Commission to further assess this issue and the safeguards that would and/or could be afforded to EEA data subjects in this context.**

4.3.1.7. Compliance risks and incompliant practices of competent Intelligence Community authorities

179. The EDPB takes note that detailed oversight reports are available. They provide for valuable elements as to what they assess as positive compliance practices, as well as to the compliance risks and incompliant practices identified.

180. In this regard, according to the IPC in its report for 2019, several elements concerning the application of the legal framework by the different competent authorities have revealed some (risks of) incompliances by the competent authorities.

181. First, the EDPB has noticed that the criteria to classify a dataset as bulk personal dataset or as targeted data do not seem to be always clear for the MI5 and SIS themselves, in particular for the MI5, which can lead to the absence of appropriate safeguards applied to the data[113]. In its report on 2019, the IPC suggested that "*this question should be resolved as a priority*"[114]. Also in relation to bulk personal datasets, the EDPB notes that for the GCHQ, although the classification of bulk personal datasets seems to be satisfying (but yet remains to be audited by the IPC), in March 2019, the internal compliance review of warrants by the dedicated team raised serious concerns, with 50% of the justifications for bulk acquisition warrants that were reviewed by the GCHQ compliance team that did not meet the required standard. According to the IPC, the compliance team had begun work to

[112] See Intelligence and Security Committee of Parliament, Privacy and Security: A modern and transparent legal framework, 2015, para. 18, p. 13, https://isc.independent.gov.uk/wp-content/uploads/2021/01/20150312_ISC_PSRptweb.pdf.
[113] See Annual Report of the Investigatory Powers Commissioner 2019, 15 December 2020, point 8.39, https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/IPC-Annual-Report-2019_Web-Accessible-version_final.pdf: "*We have observed the positive development of the [Bulk Oversight Panel (BOP)] and note its impact in managing internal compliance. We continue to seek greater clarity regarding the process MI5 uses to carry out initial examinations of new data sets to better understand decisions to classify a dataset as BPD or, for example, as targeted data. We were concerned by one unresolved action on the BOP minutes around resolving discrepancies between allocations of BPD between MI5 and SIS. It is possible, because of the different uses of the data and the different cuts of data being held, that both agencies could hold the same dataset, or versions of it, and that it could lawfully be categorised as bulk by one and targeted data by the other. There is a risk that, if one of the agencies has incorrectly categorised the data holding as targeted then that data would be held without appropriate warrant and might not be subject to appropriate safeguards.*"
[114] See Annual Report of the Investigatory Powers Commissioner 2019, point 8.39.

investigate the problem and retrain staff to improve this standard. The refreshed training on the IPA 2016 provisions and the additional training provided by policy and compliance networks (hereinafter "PCNs") have improved GCHQ's compliance in this area. The IPC does not expect to see a slip in this standard at future inspections, but will continue to review this area closely[115]. **The EDPB therefore shares the view that further review and monitoring of the said elements by the European Commission is needed as part of the assessment of the level of protection to ensure that this standard is improved, as underlined in the IPC's report, and recalls that implementation and concrete application of the legal framework shall also be taken into account as provided under Article 45 GDPR when assessing the essential equivalence of a third country.**

182. More broadly, the EDPB stresses the points of attention shared by the IPC concerning the "task-based searches" led by the MI5 officers – which allows an investigator to conduct more than one search of the bulk personal data sets available to them, and the "*serious compliance risks associated with certain technology environments in use by MI5*", concerning where data were stored in the environment, who had access to them, the extent to which they were being copied or shared, the deletion processes which applied to them, as well as concerning retention periods. Although the IPC indicates that measures have been taken and safeguards introduced, some of them remain manual and led on an individual, human-basis, it highlights that it is critical that the *"MI5 continues to maintain these new processes and to provide sufficient resources for them to function effectively. If MI5 identifies an increase in non-compliant behaviours"*[116]. The IPC expects they would be brought to its attention as soon as possible. **The EDPB therefore calls on the European Commission to closely monitor these aspects in the future**.

183. Concerning the GCHQ, the EDPB also understands from the report of the IPC that, for operations conducted under the bulk warrants, "*the quality of applications for internal approval was variable and we observed that there was room for improvement in the way that such applications were set out*"[117], and that for targeted equipment interference, the explanations for the use of general descriptors were sometimes too general and imprecise[118]. The EDPB also noticed that in the context of bulk equipment interference, the IPC recommends that "*applications should consistently and explicitly record the link between the target and a statutory purpose and intelligence requirements*"[119], that "*all applications should clearly address the potential for collateral intrusion and relevant mitigations when assessing proportionality*"[120], and that the IPC stressed that despite progress, "*there is still room for improvement*"[121] and further attention will be needed as well in the future.

184. In relation to the bulk interception regime under the Regulation of Investigatory Powers Act 2000 (hereinafter "RIPA 2000") which has since been replaced by provisions in the IPA 2016, the EDPB recalls that the insufficient oversight, both of the selection of Internet bearers for interception and the filtering, search and selection of intercepted communications for examination, was one of the core aspects that the ECtHR deemed incompliant with Article 8 ECHR with regard to the previous legislation on the investigatory powers of UK authorities in the context of national security in the *Big Brother Watch* case, now referred to the Grand Chamber. **The EDPB invites the European Commission to verify the state of play of the proceedings, to take these elements into account, and to specify them in the adequacy decision should the European Commission adopt it.**

[115] See Annual Report of the Investigatory Powers Commissioner 2019, point 10.48.
[116] See Annual Report of the Investigatory Powers Commissioner 2019, point 8.52.
[117] See Annual Report of the Investigatory Powers Commissioner 2019, point 10.2.
[118] See Annual Report of the Investigatory Powers Commissioner 2019, points 10.16 and 10.17.
[119] See Annual Report of the Investigatory Powers Commissioner 2019, point 10.23.
[120] See Annual Report of the Investigatory Powers Commissioner 2019, point 10.23.
[121] See Annual Report of the Investigatory Powers Commissioner 2019, point 10.23.

185. In this case, the ECtHR was: "*not persuaded that the safeguards governing the selection of bearers for interception and the selection of intercepted material for examination are sufficiently robust to provide adequate guarantees against abuse. Of greatest concern, however, is the absence of robust independent oversight of the selectors and search criteria used to filter intercepted communications.*"[122] As highlighted by the IPC, "*this finding echoed a similar recommendation in the Intelligence and Security Committee's Privacy and Security: A modern and transparent legal framework report of March 2015*"[123]. **The EDPB welcomes the fact that consequently, the IPC conducted a review of its approach to inspecting bulk interception in 2019, "*which included a careful review of the technically complex ways in which bulk interception is actually implemented*"[124] and committed to include "*a detailed examination of the selectors and search criteria alluded to above by the ECtHR*"[125] in the inspections of bulk interception from 2020 onwards. Given the importance of this aspect, the EDPB is concerned that a detailed examination of the selectors and search criteria by the IPC has not been carried out yet, and calls on the European Commission to closely monitor developments in this regard, especially since the concrete format of such oversight remains to be clarified[126].**

4.3.2. Further use of the information collected for national security purposes and overseas disclosure

186. When it comes to the further use of the information collected for national security purposes, the European Commission refers in its assessment to section 87(1) DPA 2018, which indeed provides that "*personal data so collected must not be processed in a manner that is incompatible with the purpose for which it is collected*". The EDPB however points out that this provision may be subject to national security exemptions as per section 110 DPA 2018. The EDPB furthermore notes that, whether for targeted interception and examination, for targeted acquisition and retention of communications data, for targeted equipment interference or for bulk interception and bulk equipment interference, the legislation provides for the possibility of "overseas disclosure".

4.3.2.1. Further use, overseas disclosure and the applicable legal framework in the UK

187. The European Commission has identified Part 4 DPA 2018, and in particular its section 109 as relevant provisions setting out specific requirements for the further use of the information collected, and notably the international transfer of personal data by intelligence services to third countries or international organisations. However, the EDPB notes that section 110 DPA 2018 provides for a national security exemption specifying that certain provisions of the DPA 2018 do not apply if exemption from these provisions is required for the purpose of safeguarding national security. The concerned provisions that may not apply include chapter 2 of Part 4 DPA 2018 in relation to the data protection principles, including purpose limitation, as well as chapter 3 of Part 4 DPA 2018 in relation to data subject rights. Section 109 DPA 2018, read in conjunction with section 110 DPA 2018 and the conditions under which it applies may lead to cases where an international transfer of personal data

[122] See ECtHR, *Big Brother Watch*, para. 347.
[123] See Annual Report of the Investigatory Powers Commissioner 2019, point 10.28.
[124] See Annual Report of the Investigatory Powers Commissioner 2019, point 10.28.
[125] See Annual Report of the Investigatory Powers Commissioner 2019, point 10.28.
[126] See Annual Report of the Investigatory Powers Commissioner 2019, point 10.28: "the exact format of this inspection is yet to be agreed".

by intelligence services to third countries takes place without applying provisions related to the data protection principles and data subject rights.

188. As identified by the European Commission, such exemption must be assessed case-by-case, and can be invoked only as far as the application of a particular provision would have negative consequences for national security. Indeed, the issuance of a national certificate for the UK intelligence services aims at certifying that an exemption is required in respect of specified personal data that are processed for the purpose of safeguarding national security. The EDPB however notes that in its guidance for national security certificate under the DPA 2018, the UK Home Office clarifies that "*[i]t is important to note from the outset that a certificate is not required in order to rely on the national security exemption; in fact, in most cases, controllers will determine for themselves whether the national security exemption is applicable.*" [127] Furthermore, the UK Home Office guidance notes that "*national security certificates may apply to personal data which can be specifically identified or cover a broader category of personal data. They may be pre-emptive as well as retrospective.*" [128] National security exemption may therefore apply in relation to an international transfer of personal data by intelligence services to third countries in the absence of a national security certificate.

189. The EDPB furthermore notes that, for example, the national security certificate DPA/S27/Security Service[129] provides that until 24 July 2024, personal data processed "*for, on behalf of, at the request of or with the aid or assistance of the Security Service or*" and "*where such processing is necessary to facilitate the proper discharge of the functions of the Security Service described in section 1 of the Security Service Act 1989*" are exempted from the corresponding provisions in UK law to Chapter V GDPR in relation to transfers of personal data to third countries or international organisations. While the other national security certificates publicly available do not provide for an exemption from the provisions of section 109 DPA 2018, it is to be recalled that some or all of the text of a national security certificate may be withheld if its publication would be against the interests of national security, would be contrary to the public interest, or might jeopardise the safety of any person.

190. In general, while assessing the draft decision in relation to these provisions, the EDPB observes that the safeguards for these disclosures solely comprise the requirement that the recipient of the data respects requirements concerning the security of data, the extent of the disclosure limited to what is necessary, the retention of data and the restriction of access to data to a limited number of persons. Thus, **the EDPB underlines that when it comes to overseas disclosures, the application of the national security exemption provided under UK law may lead to situations where safeguards ensuring that the principles of purpose limitation, necessity and proportionality, as well as the rights for the individuals, oversight and redress would not be fully provided or respected in the third country of destination. The EDPB therefore recommends the European Commission to further examine the overall safeguards provided under UK law when it comes to overseas disclosure, in particular in light of the application of national security exemptions.**

4.3.2.2. Overseas disclosure and intelligence sharing in the context of international cooperation

191. The EDPB also notes that the European Commission did not consider, as part of its adequacy assessment, existing international agreements concluded between the UK and third countries or international organisations that may provide for specific provisions for the international transfer of personal data by intelligence services to third countries.

192. The EDPB also stresses that the European Commission's assessment mainly relies on the assessment of Part 4 DPA 2018, and is notably concerned that the IPA 2016 focuses on 'requests' to exchange intelligence with foreign partners, but does not address other forms of intelligence sharing. The EDPB notes in this regard that the European Commission draft decision does not refer or assess the articulation between the UK legislative framework with the "UK-US Communication Intelligence Agreement" ("UK-US CI Agreement"). In a recent statement marking the 75th Anniversary of this agreement, the US National Security Agency (hereinafter "NSA") mentioned that this partnership allows "*to share information between the two agencies as much as possible, with minimal restrictions*" and that "*this ground-breaking document created the policies and procedures for UK and US intelligence professionals for sharing communication, translation, analysis, and code breaking information.*" [130] This agreement also became the foundation for other intelligence partnership with Australia, Canada, and New Zealand.

193. The secret nature of this agreement and its specific provisions raise a serious challenge in terms of clarity and foreseeability of the law in relation to the further use and overseas disclosure of information collected by UK authorities for national security purposes. In this context, the EDPB recalls that when it comes to the level of protection guaranteed within the EU, the CJEU has stressed that legislation involving interference with the fundamental right to the protection of personal data must "*lay down clear and precise rules governing the scope and application of a measure and imposing minimum safeguards, so that the persons whose personal data is concerned have sufficient guarantees enabling their data to be effectively protected against the risk of abuse and against any unlawful access and use of that data. The need for such safeguards is all the greater where personal data is subjected to automatic processing and where there is a significant risk of unlawful access to that data*"[131]. The EDPB therefore considers that the European Commission should consider the impact of the UK-US CI Agreement as part of its adequacy assessment.

194. The ECtHR, in its first section judgment of 13 September 2018, in the *Big Brother Watch* case, has assessed the UK intelligence sharing regime and in particular the UK-US CIAgreement. The ECtHR indeed stated that "*[t]he statutory framework which permits the United Kingdom intelligence services to request intercepted material from foreign intelligence agencies is not contained in RIPA. The British-US Communication Intelligence Agreement of 5 March 1946 specifically permits the exchange of material between the United States and the United Kingdom*"[132] and considered that there is "*a basis in law for the requesting of intelligence from foreign intelligence agencies, and that that law is sufficiently accessible.*"[133] While the ECtHR has concluded that there has been no violation of Article 8[134] ECHR in relation to the intelligence sharing regime, the EDPB notes that this judgment has now been referred to the Grand Chamber which decision is still pending. The EDPB also notes that in a partly concurring, partly dissenting opinion to this judgment, Judge Koskelo, joined by Judge

[127] See Home Office, The Data Protection Act 2018, National Security Certificates guidance, August 2020, para 3, p. 3.
[128] See Home Office, The Data Protection Act 2018, National Security Certificates guidance, August 2020, para 5, p. 4.
[129] See DPA/S27/Security Service, section 27 DPA 2018, Certificate of the Secretary of State, 24 July 2019, https://ico.org.uk/media/about-the-ico/documents/nscs/2615660/nsc-part-2-mi5-201908.pdf.

[130] See NSA's press release, GCHQ and NSA Celebrate 75 Years of Partnership, 5 February 2021, https://www.nsa.gov/News-Features/Feature-Stories/Article-View/Article/2494453/gchq-and-nsa-celebrate-75-years-of-partnership/.
[131] See *Schrems I*, para. 91.
[132] See ECtHR, *Big Brother Watch*, para. 425.
[133] See ECtHR, *Big Brother Watch*, para. 427.
[134] See ECtHR, *Big Brother Watch*, para. 448.

Turković[135], has concluded that there is a violation of Article 8 ECHR in relation to the intelligence sharing regime, stating that "*[i]t is easy to agree with the principle that any arrangement under which intelligence from intercepted communications is obtained via foreign intelligence services, whether on the basis of requests to carry out such interception or to convey its results, should not be allowed to entail a circumvention of the safeguards which must be in place for any surveillance by domestic authorities (see paragraphs 216, 423 and 447). Indeed, any other approach would be implausible*".

195. As highlighted by several reports from the media and non-governmental organisations[136][137], the most recent version of the UK-US CI Agreement to have been made public dates back from 1956 and since then, communication technology and the nature of signals intelligence have changed significantly. Media reports have for example revealed that data transiting through undersea cables that land in the UK are intercepted by the GCHQ and made accessible to the NSA[138].

196. For the EDPB, a key question in relation to intelligence sharing is whether section 109 DPA 2018 and the provisions of the IPA 2016 remain applicable when UK intelligence services act in accordance with the UK-US CI Agreement. Another key element to be assessed is whether the provisions or effective application of this agreement impact on the level of protection of personal data in transit from the EEA to the UK, or allows for a direct access and acquisition of personal data by other third countries intelligence services.

197. Consequently, in addition to reservations expressed as to "overseas disclosures" on the basis of Part 4 DPA 2018 and its related national security exemption, as well as of requests in the framework of the IPA 2016, **the EDPB is concerned about other forms of information-sharing and disclosures, on the basis of other instruments, in particular the various international agreements concluded by the UK with other third countries, especially where these instruments remain inaccessible to the public, such as the UK-US CI Agreement. The effect of such agreement could lead to a circumvention of the safeguards identified in relation to the access and use of personal data for national security purposes.**

198. Indeed, the EDPB shares the view expressed by Special Rapporteur to the United Nations, Joe Cannatacci, that "*[i]ntelligence sharing must not result in a backdoor to obtain or facilitate for others the obtaining of intelligence free from domestic safeguards, nor a loophole for foreign Governments with lower standards on the protection of privacy (or other human rights) to obtain intelligence from UK intelligence that could give rise to human rights violations*"[139].

199. Furthermore, **the EDPB considers that the conclusion of bilateral or multilateral agreements with third countries for the purpose of intelligence cooperation, providing a legal basis for direct interception and acquisition of personal data or the transfer of personal data to these countries may also significantly affect the conditions for further use of the information collected, since such agreements are likely to affect the UK data protection legal framework as assessed.**

[135] See ECtHR, *Big Brother Watch*, partly concurring, partly dissenting opinion of Judge Koskelo, joined by Judge Turković.
[136] See BBC, Diary reveals birth of secret UK-US spy pact that grew into Five Eyes, 5 March 2021, https://www.bbc.com/news/uk-56284453.
[137] See Privacy International, Policy Briefing - UK Intelligence Sharing Arrangements, April 2018, https://privacyinternational.org/sites/default/files/2018-04/Privacy%20International%20Briefing%20-%20Intelligence%20Sharing%20%28UK%29%20FINAL.pdf.
[138] See The Guardian, GCHQ taps fibre-optic cables for secret access to world's communications, 21 June 2013, https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.
[139] See End of Mission Statement of the Special Rapporteur on the Right to Privacy at the Conclusion Of his Mission to the United Kingdom of Great Britain and Northern Ireland, London, 29 June 2018, https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23296&LangID=E#:~:text=Intelligence%20sharing%20must%20not%20result,UK%20intelligence%20that%20could%20give.

4.3.3. Oversight

200. The EDPB emphasises the importance of comprehensive supervision by independent supervisory authorities for an adequate level of data protection. The guarantee of independence within the meaning of Article 8(3) EU Charter of the supervisory authorities is intended to ensure effective and reliable monitoring of compliance with the rules on the protection of individuals with regard to the processing of personal data.

201. When personal data are accessed and used for national security purposes, the oversight function is mainly fulfilled by the IPC and the Judicial Commissioners (hereinafter the "Judicial Commissioners").

202. **The EDPB generally recognises the introduction of Judicial Commissioners in the IPA 2016 as a significant improvement.** In line with a request above, the European Commission is invited to assess the independence of the **Judicial Commissioners in more detail, and in particular to what extent the independence of the IPC and the IPC's office (hereinafter "IPCO") is legally secured, as such is not found in the IPA 2016.** This is even more important as the IPC decides on appeals by the government, in case an application for a surveillance **measure** has been denied **by** a judicial commissioner.

203. The IPC has *ex-ante*, as well as *ex-post* oversight functions. As regards *ex-ante* oversight, the EDPB understands that the function of the Judicial Commissioners is to approve, in individual cases, different surveillance measures, including targeted interception and bulk acquisition of communication data. The EDPB further notes that prior-approval of surveillance measures cannot be derived from the jurisprudence of the CJEU as an absolute requirement for the proportionality of surveillance measures.[140]

204. In order to assess the effectiveness of this level of oversight, the EDPB nevertheless sees the need to further clarify the scenarios for which a lawful interception without a prior-approval of the Judicial Commissioners is possible.

205. In its draft decision, the European Commission mentions in footnotes 201 and 266 "specific limited cases" provided by the IPA 2016 in its sections 44 to 52 with regard to targeted interceptions. The EDPB notes that sections 45 - 51 IPA 2016 are exemptions that are claimed not to be regularly used by intelligence services. Furthermore, the **EDPB understands** that in the **cases where the exemptions apply** (e.g. telecommunications and postal providers), the prior-approval carried out by the Judicial Commissioners is to be conducted in the event that law enforcement authorities or intelligence services **request** access to these data**, and invites the European Commission to confirm in its decision that this is correct**.

206. The EDPB recognises that section 44(2) IPA 2016 permits interception of communications if one of the parties (sender or recipient) has consented and there is an authorisation under the RIPA 2000 or the Regulation of Investigatory Powers (Scotland) Act 2000 (2000 asp 11), i.e. the former legal situation before the establishment of the Judicial Commissioners. The EDPB **invites** the European

[140] It also notes, however, that the CJEU, when invalidating the Privacy Shield in *Schrems II*, has taken note of the fact that, under US law, the so called FISA Court "*does not authorise individual surveillance measures; rather, it authorises surveillance programs (like PRISM, UPSTREAM) on the basis of annual certifications*"." (para. 179).

Commission to clarify whether this means that in cases where a unilateral consent exists, the prior-approval procedure would not apply at all.

207. As regards *ex-post* oversight, it is also important to verify that efficient independent oversight is ensured without gaps, in particular where it is not foreseen *ex-ante*.

208. The EDPB notes that for the sections 48 - 52 IPA 2016, an *ex-post* review by the Judicial Commissioners takes place, and **invites the European Commission to clarify under which requirements and on whose initiative such an *ex-post* review is to be conducted**.

209. According to section 229(4) IPA 2016, the IPC is not to keep under review the exercise of certain functions. In this regard the EDPB invites the European Commission to clarify the provisions of section 229(4)(d) and (e) IPA 2016 regarding its practical impact on the review competence of the IPC. **It is the understanding of the EDPB that the ICO is the competent oversight authority where the exemptions of section 229(4) IPA 2016 apply, and the EDPB invites the European Commission to confirm in its decision that this is correct.**

210. **It appears that, when conducting** *ex-post* oversight**, the IPC's** role is **limited** to make recommendations in cases of non-compliance, and to give notice to the data subject, if the error is serious and it is in the public interest for the person to be informed. **The EDPB invites the European Commission to clarify how the IPCO can effectively ensure compliance with the law.**

211. **Finally, the EDPB understands that affected individuals cannot directly address the IPCO, but must lodge a complaint with the ICO, which, however, has limited competences in the area of national security. The EDPB therefore invites the European Commission to further clarify how it is legally ensured that the IPCO addresses complaints in these cases.**

4.3.4. Redress

212. In the light of the *Schrems I* and *Schrems II* judgments by the CJEU, it is clear that effective judicial protection in the meaning of Article 47 EU Charter is of fundamental importance for the assumption of adequacy of the law of a third country. The rulings have also shown that particular attention, in this regard, has to be paid to effective judicial protection in the area of national security access to personal data.

213. **The EDPB recognises that the UK has established the IPT. The IPT is not only competent to hear cases on the use of investigatory powers by law enforcement authorities, but also by intelligence services. It is the understanding of the EDPB that the IPT functions as a proper court in the meaning of Article 47 EU Charter. As to its powers, the European Commission is invited to confirm that the IPT has all those powers mentioned in recital 262 of the draft decision, regardless of the legal basis under which the complaint is brought.**

214. Discreet surveillance by intelligence agencies will often mean that the object of the surveillance, the data subject, is and will not be aware of the surveillance. In this context, when it had to analyse US law, the EDPB has many times expressed its concern with the requirement of "standing", as interpreted in US law, in surveillance cases. Against this background, the EDPB notes that the complaint with the IPT only requires a "belief" test, according to which the complainant has to show she or he is potentially at risk of being subjected to a measure.

215. When analysing the IPT, the EDPB also pays particular attention to the fact that the functioning of the IPT has been repeatedly found to be in compliance with the ECHR, as interpreted by the ECtHR.



Opinia nr 3/2019 w sprawie pytań i odpowiedzi dotyczących wzajemnych zależności między rozporządzeniem w sprawie badań klinicznych (RBK) a ogólnym rozporządzeniem o ochronie danych (RODO) (art. 70 ust. 1 lit. b))

Przyjęta w dniu 23 stycznia 2019 r.

Spis treści

1 Wprowadzenie 3

2 Podstawa prawna przetwarzania danych osobowych w okresie objętym protokołem badania klinicznego (pierwotne wykorzystanie) 4

2.1 Operacje przetwarzania związane z celami dotyczącymi wiarygodności i bezpieczeństwa ... 5

2.2 Operacje przetwarzania związane wyłącznie z działalnością badawczą 5

3 Wtórne wykorzystywanie danych pochodzących z badań klinicznych poza protokołem badania klinicznego do celów naukowych 8

4 Podsumowanie 9

Europejska Rada Ochrony Danych,

uwzględniając art. 70 ust. 1 lit. b) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (zwanego dalej „RODO"),

uwzględniając Porozumienie EOG, w szczególności załącznik XI i protokół 37 do tego Porozumienia, zmienione decyzją Wspólnego Komitetu EOG nr 154/2018 z dnia 6 lipca 2018 r.,

uwzględniając art. 12 i 22 swojego regulaminu z dnia 25 maja 2018 r.,

PRZYJMUJE NINIEJSZĄ OPINIĘ:

1 WPROWADZENIE

1. W dniu 8 października 2018 r. Komisja Europejska (DG SANTE) zwróciła się do Europejskiej Rady Ochrony Danych (EROD) o konsultacje – zgodnie z art. 70 ogólnego rozporządzenia o ochronie danych – w sprawie dokumentu pt. „Pytania i odpowiedzi dotyczące wzajemnych zależności między rozporządzeniem w sprawie badań klinicznych (RBK)[1] a ogólnym rozporządzeniem o ochronie danych (RODO)[2]" (zwanego dalej „pytaniami i odpowiedziami").
2. RODO zapewnia ochronę osób fizycznych w związku z przetwarzaniem danych osobowych oraz zharmonizowane przepisy dotyczące swobodnego przepływu takich danych, zaś celem RBK jest zapewnienie większej harmonizacji przepisów w zakresie prowadzenia badań klinicznych w całej UE. Ustanowiono w nim w szczególności procedurę wydawania pozwolenia na podstawie jednego wniosku za pośrednictwem jednego portalu UE, procedurę oceny prowadzącą do wydania jednej decyzji, przepisy dotyczące ochrony osób fizycznych oraz wymogi dotyczące świadomej zgody i przejrzystości.
3. Należy przypomnieć, że RBK weszło w życie z dniem 16 czerwca 2014 r., lecz termin rozpoczęcia jego stosowania został przesunięty, ponieważ zależy on od stworzenia w pełni funkcjonalnych portalu i bazy danych UE dotyczących badań klinicznych. RBK zacznie być stosowane dopiero po przeprowadzeniu niezależnego audytu oraz po upływie 6 miesięcy od opublikowania zawiadomienia potwierdzającego przez Komisję Europejską. W związku z tym obecnie szacuje się, że stosowanie rozporządzenia rozpocznie się w 2020 r.
4. Należy ponadto zauważyć, iż art. 93 RBK stanowi, że „państwa członkowskie stosują dyrektywę 95/46/WE [obecnie uchyloną ogólnym rozporządzeniem o ochronie danych] do przetwarzania danych osobowych, które odbywa się w państwach członkowskich na podstawie niniejszego rozporządzenia" oraz że „rozporządzenie (WE) nr 45/2001 [uchylone rozporządzeniem 2018/1725] stosuje się do przetwarzania danych osobowych przez Komisję i Agencję na podstawie niniejszego

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 536/2014 z dnia 16 kwietnia 2014 r. w sprawie badań klinicznych produktów leczniczych stosowanych u ludzi oraz uchylenia dyrektywy 2001/20/WE, Dz.U. L 158 z 27.5.2014.

[2] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), Dz.U. L 119 z 4.5.2016.

rozporządzenia". RODO również zawiera wyraźne odniesienia do odpowiednich przepisów mających zastosowanie do badań klinicznych[3]. Z powyższego wynika, że obydwa te akty prawne mają zastosowanie jednocześnie oraz że RBK ma charakter prawa sektorowego zawierającego przepisy szczegółowe istotne z punktu widzenia ochrony danych, ale nie ustanawia ono żadnych odstępstw od RODO.

5. Aby zapewnić wytyczne dotyczące spójnego podejścia do ochrony danych w badaniach klinicznych w UE, w pytaniach i odpowiedziach Komisja Europejska odniosła się do szeregu zagadnień, które – z wyjątkiem pytania 11 mającego na celu wyjaśnienie obecnej sytuacji zgodnie z dyrektywą w sprawie badań klinicznych – będą miały większe znaczenie, gdy RBK zacznie być stosowane. Zagadnienia te obejmują: odpowiednią podstawę prawną, świadomą zgodę i jej wycofanie, informacje na temat osób, których dane dotyczą, przekazywanie i wtórne wykorzystywanie danych. Chociaż RBK nie ma jeszcze zastosowania, informacje zawarte w tych często zadawanych pytaniach stanowią dobrą podstawę do badań klinicznych zgodnych z RODO.
6. EROD zdaje sobie sprawę z pilnej potrzeby zapewnienia wyjaśnień, w szczególności po wejściu w życie RODO, i postanowiła skoncentrować swoje uwagi dotyczące projektu pytań i odpowiedzi na kwestiach odpowiedniej podstawy prawnej przetwarzania danych osobowych w kontekście badań klinicznych (pierwotne wykorzystanie) oraz wtórnego wykorzystania danych pochodzących z badań klinicznych do innych celów naukowych.

2 PODSTAWA PRAWNA PRZETWARZANIA DANYCH OSOBOWYCH W OKRESIE OBJĘTYM PROTOKOŁEM BADANIA KLINICZNEGO (PIERWOTNE WYKORZYSTANIE)

7. W kontekście niniejszej opinii EROD uważa, że wszystkie operacje przetwarzania związane z konkretnym protokołem badania klinicznego w całym okresie objętym tym protokołem – od rozpoczęcia badania do usunięcia danych po zakończeniu okresu archiwizacji – należy rozumieć jako pierwotne wykorzystanie danych pochodzących z badań klinicznych[4]. EROD uważa jednak, że nie wszystkie operacje przetwarzania odnoszące się do takiego „pierwotnego wykorzystania" danych pochodzących z badań klinicznych służą tym samym celom i podlegają tej samej podstawie prawnej.
8. Ogólnym celem RBK jest urzeczywistnienie zharmonizowanego rynku wewnętrznego w odniesieniu do badań klinicznych i produktów leczniczych stosowanych u ludzi, mając za podstawę wysoki poziom ochrony zdrowia, przy jednoczesnym ustanowieniu wysokich norm jakości i bezpieczeństwa produktów leczniczych poprzez zapewnienie wiarygodności i odporności danych uzyskanych w badaniach klinicznych[5].
9. Zdaniem EROD przy omawianiu kwestii podstawy prawnej przetwarzania danych osobowych w całym okresie objętym badaniem klinicznym istotne jest, by rozróżnić dwie główne kategorie czynności przetwarzania. W szczególności operacje przetwarzania związane wyłącznie z działalnością badawczą należy odróżnić od operacji przetwarzania związanych z celami dotyczącymi ochrony zdrowia, ustanawiając jednocześnie normy jakości i bezpieczeństwa produktów leczniczych przez generowanie wiarygodnych i odpornych danych (cele dotyczące wiarygodności i bezpieczeństwa); do tych dwóch głównych kategorii czynności przetwarzania mają zastosowanie różne podstawy prawne.

2.1 Operacje przetwarzania związane z celami dotyczącymi wiarygodności i bezpieczeństwa

10. Zdaniem EROD można uznać, że operacje przetwarzania wyraźnie przewidziane w RBK i w odpowiednich przepisach krajowych oraz związane z celami dotyczącymi wiarygodności i bezpieczeństwa wchodzą w zakres pojęcia „obowiązku prawnego ciążącego na administratorze" w rozumieniu art. 6 ust. 1 lit. c) RODO.
11. Grupa Robocza Art. 29[6] omówiła warunki, na jakich ta podstawa prawna może mieć zastosowanie: obowiązek ten musi zostać nałożony przepisami prawa; przepisy te muszą spełniać wszystkie istotne warunki, aby obowiązek był ważny i wiążący; przepisy te muszą być zgodne przepisami o ochronie danych, w tym z wymogiem konieczności, proporcjonalności i ograniczenia celu; sam obowiązek prawny musi być wystarczająco jasny co do wymaganego na jego mocy przetwarzania danych osobowych; administrator nie powinien dysponować nadmierną swobodą uznania w zakresie sposobu wywiązania się z obowiązku prawnego. EROD uważa, że dotyczy to w szczególności obowiązków związanych ze zgłaszaniem danych dotyczących bezpieczeństwa w rozumieniu art. 41–43 RBK, a także obowiązków związanych z archiwizacją podstawowej dokumentacji badania klinicznego (25 lat zgodnie z art. 58 RBK) i dokumentacji medycznej uczestników (obowiązki te należy określić w prawie krajowym zgodnie z tym samym przepisem). Ta sama zasada dotyczy wszelkiego ujawniania danych pochodzących z badań klinicznych właściwym organom krajowym w trakcie inspekcji zgodnie z odpowiednimi przepisami krajowymi (zob. art. 77–79 RBK).
12. W związku z tym przetwarzanie danych osobowych w kontekście zgłaszania danych dotyczących bezpieczeństwa lub w kontekście inspekcji przeprowadzanej przez właściwy organ krajowy bądź zatrzymywanie danych pochodzących z badań klinicznych w ramach wykonywania obowiązków w zakresie archiwizacji ustanowionych rozporządzeniem w sprawie badań klinicznych lub, w stosownych przypadkach, odpowiednimi przepisami krajowymi, należy uznać za niezbędne do wywiązania się z obowiązków prawnych spoczywających na sponsorze lub badaczu.
13. Właściwym warunkiem zgodnego z prawem przetwarzania szczególnych kategorii danych w kontekście tych obowiązków jest zatem warunek określony w art. 9 ust. 2 lit. i): „przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak […] zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa państwa członkowskiego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową".

2.2 Operacje przetwarzania związane wyłącznie z działalnością badawczą[7]

[3] Motywy 156 i 161 RODO.
[4] Należy zauważyć, że tego rodzaju wykładnia rozszerzająca pojęcia pierwotnego wykorzystania danych różni się od koncepcji pierwotnego wykorzystania przyjętej w opinii Grupy Roboczej Art. 29 nr 3/2013 z dnia 3 kwietnia 2013 r. w sprawie ograniczenia celu, WP 203, s. 21, w której stwierdzono, że pierwsza operacja przetwarzania, tj. gromadzenie danych, stanowi pierwotne wykorzystanie, natomiast wszelkie przetwarzanie po zgromadzeniu danych należy uznać za „dalsze przetwarzanie".
[5] Motyw 82 RBK i art. 3 lit. b) RBK.
[6] Opinia 6/2014 w sprawie pojęcia uzasadnionych interesów administratora danych zawartego w art. 7 dyrektywy 95/46/WE, przyjęta dnia 9 kwietnia 2014 r., WP 217, p. 19.
[7] W wytycznych Grupy Roboczej Art. 29 dotyczących zgody na mocy rozporządzenia 2016/679 z dnia 10 kwietnia 2018 r., s. 27 stwierdzono, że pojęcia badań naukowych nie można rozciągać poza jego powszechne znaczenie i że „badania naukowe" w tym kontekście oznaczają projekt badawczy utworzony zgodnie z odpowiednią metodyką sektorową i etycznymi standardami, a także dobrą praktyką.

14. Operacje przetwarzania związane wyłącznie z działalnością badawczą w kontekście badania klinicznego nie mogą jednak wynikać z obowiązku prawnego. W zależności od wszystkich okoliczności badania i konkretnej czynności przetwarzania danych działalność badawcza może być objęta zakresem stosowania przepisów dotyczących wyraźnej zgody osoby, której dane dotyczą (art. 6 ust. 1 lit. a) w związku z art. 9 ust. 2 lit. a)), zadania realizowanego w interesie publicznym (art. 6 ust. 1 lit. e)) albo prawnie uzasadnionych interesów administratora (art. 6 ust. 1 lit. f) w związku z art. 9 ust. 2 lit. i) lub j) RODO).

Zgoda – wyraźna zgoda

15. Jak słusznie wskazano w pkt 4 pytań i odpowiedzi, *świadomej zgody* przewidzianej w RBK nie można mylić z pojęciem zgody jako podstawy prawnej przetwarzania danych osobowych zgodnie z RODO.
16. Przepisy rozdziału V RBK w zakresie *świadomej zgody*, w szczególności jego art. 28, odpowiadają przede wszystkim podstawowym wymogom etycznym dotyczącym projektów badawczych z udziałem ludzi, wynikającym z deklaracji helsińskiej. Obowiązek uzyskania *świadomej zgody* uczestników badania klinicznego służy przede wszystkim zapewnieniu ochrony prawa do godności ludzkiej i prawa do integralności osoby zgodnie z art. 1 i 3 Karty praw podstawowych Unii Europejskiej; nie ma on stanowić instrumentu zapewniającego przestrzeganie przepisów o ochronie danych osobowych.
17. Zgodnie z RODO zgoda musi być dobrowolna, konkretna, świadoma i jednoznaczna, przy czym w przypadku przetwarzania szczególnych kategorii danych, takich jak dane dotyczące zdrowia, wymagana jest *wyraźna zgoda* (art. 9 ust. 2 lit. a) RODO). Aby ocenić, czy *wyraźna zgoda* danej osoby może być ważną podstawą prawną przetwarzania danych wrażliwych w trakcie badania klinicznego, administratorzy danych powinni należycie uwzględnić wytyczne Grupy Roboczej Art. 29 dotyczące zgody oraz sprawdzić, czy wszystkie warunki udzielenia ważnej zgody mogą zostać spełnione, biorąc pod uwagę konkretne okoliczności tego badania[8].
18. Zdaniem EROD administratorzy danych powinni zwracać szczególną uwagę na warunek „dobrowolności" zgody. Jak stwierdzono w wytycznych Grupy Roboczej Art. 29 dotyczących zgody, element ten oznacza zapewnienie osobom, których dane dotyczą, faktycznej możliwości wyboru i kontroli. Ponadto zgoda nie powinna stanowić ważnej podstawy prawnej przetwarzania danych osobowych w szczególnym przypadku, w którym występuje wyraźny brak równowagi między osobą, której dane dotyczą, a administratorem[9].
19. Zależnie od okoliczności badania klinicznego może wystąpić brak równowagi sił między sponsorem/badaczem a uczestnikami. W RBK wyraźnie odniesiono się do tych zagrożeń i nałożono na badacza obowiązek wzięcia pod uwagę wszystkich istotnych okoliczności, a w szczególności kwestii, czy potencjalny uczestnik należy do grupy gorzej sytuowanej pod względem ekonomicznym lub społecznym lub znajduje się w sytuacji zależności instytucjonalnej lub hierarchicznej, która mogłaby w niewłaściwy sposób wpłynąć na jego decyzję o udziale[10].
20. Należy jednak pamiętać, że nawet w przypadku gdy warunki uzyskania *świadomej zgody* zgodnie z RBK zostaną spełnione, wyraźny brak równowagi sił między uczestnikiem a sponsorem/badaczem sprawi, że zgoda nie będzie „dobrowolna" w rozumieniu RODO.

[8] Wytyczne Grupy Roboczej Art. 29 dotyczące zgody na mocy rozporządzenia 2016/679 z dnia 10 kwietnia 2018 r., zatwierdzone przez EROD w dniu 25 maja 2018 r.
[9] *Idem*, s. 6. Zob. również motyw 43 RODO.
[10] Motyw 31 RBK.

Zdaniem EROD taka sytuacja będzie miała miejsce na przykład wówczas, gdy uczestnik zmaga się z problemami zdrowotnymi, gdy uczestnicy należą do grupy gorzej sytuowanej pod względem ekonomicznym lub społecznym bądź znajdują się w sytuacji jakiejkolwiek zależności instytucjonalnej lub hierarchicznej. W związku z tym, jak wyjaśniono w wytycznych dotyczących zgody Grupy Roboczej Art. 29, w większości przypadków zgoda nie będzie właściwą podstawą prawną – należy się wówczas opierać na innych podstawach prawnych (zob. alternatywne podstawy prawne omówione poniżej).

21. W związku z tym EROD uważa, że administratorzy danych powinni szczególnie dokładnie ocenić okoliczności badania klinicznego, zanim uznają zgodę osoby za podstawę prawną przetwarzania danych osobowych do celów prowadzenia działalności badawczej w ramach tego badania.

Wycofanie zgody

22. Biorąc pod uwagę warunki udzielenia zgody określone w obydwu omawianych aktach prawnych, EROD uważa, że nie należy mylić wycofania *świadomej zgody* w rozumieniu art. 28 ust. 3 RBK z wycofaniem zgody w rozumieniu RODO. W RBK wyraźnie przewidziano, że wycofanie świadomej zgody, które nie ma wpływu na działania już przeprowadzone w oparciu o świadomą zgodę przed jej wycofaniem ani na wykorzystanie danych uzyskanych przed jej wycofaniem, pozostaje „[b]ez uszczerbku dla dyrektywy 95/46/WE" (obecnie RODO).
23. Zgodnie z RODO, jeżeli zgoda jest używana jako zgodna z prawem podstawa przetwarzania, musi istnieć możliwość wycofania tej zgody w dowolnym momencie (art. 7 ust. 3), przy czym nie ustanowiono wyjątku od tego wymogu w odniesieniu do badań naukowych[11]. Co do zasady w przypadku wycofania zgody wszystkie operacje przetwarzania danych, które były oparte na zgodzie, pozostają zgodne z prawem zgodnie z RODO (art. 7 ust. 3); administrator przerywa jednak dane czynności przetwarzania i jeżeli nie istnieje żadna inna zgodna z prawem podstawa uzasadniająca zatrzymanie danych do dalszego przetwarzania, administrator powinien je usunąć (zob. art. 17 ust. 1 lit. b) i art. 17 ust. 3 RODO).
24. W związku z tym przy zastosowaniu wycofania zgody – zgodnie z art. 7 RODO – na przetwarzanie danych osobowych do celów badawczych konieczne jest uwzględnienie innych celów przetwarzania w oparciu o innego rodzaju zgodne z prawem podstawy. W kontekście badań klinicznych zgoda osoby, której dane dotyczą, ogranicza się do operacji przetwarzania związanych wyłącznie z działalnością badawczą. Oznacza to, że w przypadku wycofania zgody przez osobę wszystkie działania badawcze prowadzone z wykorzystaniem danych pochodzących z badań klinicznych dotyczących tej osoby zostają zakończone. Wycofanie zgody pozostaje jednak bez uszczerbku dla operacji przetwarzania opartych na innych zgodnych z prawem podstawach, w szczególności na obowiązkach prawnych ciążących na sponsorze/badaczu, takich jak obowiązki związane z bezpieczeństwem (zob. pkt 1.1 powyżej).

Zadania realizowane w interesie publicznym lub z uwagi na prawnie uzasadniony interes administratora

25. Zdaniem EROD jako wariant alternatywny dla zgody osoby, której dane dotyczą, właściwsze są zgodne z prawem podstawy przetwarzania przewidziane w art. 6 ust. 1 lit. e) lub w art. 6 ust. 1 lit. f).

[11] Grupa Robocza Art. 29, Wytyczne dotyczące zgody na mocy rozporządzenia 2016/679, 28 listopada 2017 r., WP 259.

26. Przetwarzanie danych osobowych przez administratorów danych można uznać za „niezbędne do wykonania zadania realizowanego w interesie publicznym" zgodnie z art. 6 ust. 1 lit. e) RODO. Art. 6 ust. 3 RODO stanowi ponadto, że podstawa ta musi być określona w prawie Unii lub w prawie państwa członkowskiego oraz że cel przetwarzania musi być określony w tej podstawie prawnej. Przetwarzanie danych osobowych w kontekście badań klinicznych można zatem uznać za niezbędne do wykonania zadania realizowanego w interesie publicznym, jeżeli prowadzenie badań klinicznych wchodzi bezpośrednio w zakres upoważnienia, misji oraz zadań powierzonych podmiotowi publicznemu lub prywatnemu na mocy prawa krajowego[12].
27. We wszystkich innych sytuacjach, w których prowadzenie badań klinicznych nie może zostać uznane za niezbędne do wykonywania zadań realizowanych w interesie publicznym powierzonych administratorowi na mocy prawa, EROD uzna, że przetwarzanie danych osobowych może być „niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą" – zgodnie z art. 6 ust. 1 lit. f) RODO.
28. W odniesieniu do przetwarzania szczególnych kategorii danych podstawa prawna określona w art. 6 ma zastosowanie jedynie wówczas, gdy art. 9 RODO przewiduje szczególne odstępstwo od ogólnego zakazu przetwarzania szczególnych kategorii danych. EROD uważa, że w zależności od konkretnych okoliczności badania klinicznego właściwym warunkiem w rozumieniu art. 9 w odniesieniu do wszystkich operacji przetwarzania danych wrażliwych do celów czysto badawczych mogą być „względy związane z ważnym interesem publicznym w dziedzinie zdrowia publicznego [...] na podstawie prawa państwa członkowskiego" (art. 9 ust. 2 lit. i)) albo „cele badań naukowych [...] zgodnie z art. 89 ust. 1, na podstawie prawa Unii lub prawa państwa członkowskiego" (art. 9 ust. 2 lit. j)).

3 WTÓRNE WYKORZYSTYWANIE DANYCH POCHODZĄCYCH Z BADAŃ KLINICZNYCH POZA PROTOKOŁEM BADANIA KLINICZNEGO DO CELÓW NAUKOWYCH

29. Kwestia wtórnego wykorzystywania została wyszczególniona w art. 28 ust. 2 RBK, ze szczególnym uwzględnieniem zgody. W artykule tym jest mowa wyłącznie o sytuacjach, w których sponsor pragnie przetwarzać dane uczestnika badania klinicznego „poza protokołem badania klinicznego", lecz tylko i „wyłącznie" do celów naukowych. W RBK stwierdzono, że o wyrażenie zgody na ten konkretny cel przetwarzania należy zwrócić się do osoby, której dane dotyczą, lub jej wyznaczonego zgodnie z prawem przedstawiciela w chwili zwrócenia się o wyrażenie świadomej zgody na udział w badaniu klinicznym. Jak wskazano powyżej w odniesieniu do przepisów rozdziału V RBK dotyczących *świadomej zgody*, zgoda przewidziana w art. 28 ust. 2 RBK nie jest jednak równoważna zgodzie, o której mowa w RODO jako o jednej z podstaw prawnych przetwarzania danych osobowych, niezależnie od tego, czy jest to podstawa prawna zastosowana do pierwotnego przetwarzania.
30. W związku z tym, jak podkreśla Komisja Europejska w pytaniach i odpowiedziach, a dokładnie w pytaniu nr 7, jeżeli sponsor lub badacz chcieliby dalej wykorzystywać zgromadzone dane osobowe do jakichkolwiek innych celów naukowych niż cele określone w protokole badania klinicznego, wymagałoby to innej szczególnej podstawy prawnej niż ta, którą zastosowano do pierwotnego celu. Wybrana podstawa prawna może, lecz nie musi się różnić od podstawy prawnej pierwotnego wykorzystania.
31. EROD uważa jednak, że takie podejście wyklucza w każdym przypadku możliwość zastosowania tzw. domniemania zgodności przewidzianego w art. 5 ust. 1 lit. b) RODO. Artykuł ten stanowi, że dalsze przetwarzanie danych do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest *a priori* uznawane za niezgodne z pierwotnym celem, pod warunkiem że jest ono zgodne z przepisami art. 89, który przewiduje w tych przypadkach konkretne odpowiednie zabezpieczenia i wyjątki. W takim przypadku administrator mógłby, pod pewnymi warunkami, dalej przetwarzać dane bez potrzeby powoływania się na nową podstawę prawną[13]. Warunki te, ze względu na ich horyzontalny i złożony charakter, będą w przyszłości wymagały szczególnej uwagi i szczególnych wskazówek ze strony EROD. Póki co domniemania zgodności, z zastrzeżeniem warunków określonych w art. 89, nie należy wykluczać w każdym przypadku w odniesieniu do wtórnego wykorzystania danych pochodzących z badań klinicznych poza protokołem badania klinicznego do innych celów naukowych.
32. W każdym razie, nawet jeżeli domniemanie zgodności będzie miało zastosowanie, badania naukowe wykorzystujące dane poza protokołem badania klinicznego należy prowadzić zgodnie ze wszystkimi innymi właściwymi, mającymi zastosowanie przepisami dotyczącymi ochrony danych zgodnie z art. 28 ust. 2 RBK. W związku z tym uznaje się, że administrator nie jest zwolniony z pozostałych obowiązków wynikających z przepisów o ochronie danych, na przykład w odniesieniu do rzetelności, zgodności z prawem (tj. zgodnie z mającym zastosowanie prawem unijnym i krajowym), konieczności i proporcjonalności, a także jakości danych.

4 PODSUMOWANIE

33. Podsumowując, EROD zaleca zmodyfikowanie pytań i odpowiedzi w części, w której jest mowa o zgodnych z prawem podstawach przetwarzania, aby odróżnić czynności przetwarzania związane z wiarygodnością i bezpieczeństwem, które wynikają bezpośrednio z obowiązków prawnych administratora i które podlegają podstawie prawnej określonej w art. 6 ust. 1 lit. c) w związku z art. 9 ust. 1 lit. i) RODO.
34. W odniesieniu do wszystkich innych czynności przetwarzania, określonych w niniejszej opinii jako operacje przetwarzania związane wyłącznie z działalnością badawczą, pytania i odpowiedzi należy zmienić tak, aby odzwierciedlały one trzy alternatywne podstawy prawne, w zależności od wszystkich okoliczności konkretnego badania klinicznego:

    - zadanie realizowane w interesie publicznym zgodnie z art. 6 ust. 1 lit. e) w związku z art. 9 ust. 2 lit. i) lub j) RODO;

[12] Zgodnie z motywem 45 RODO nie nakłada się w nim wymogu, aby dla każdego indywidualnego przetwarzania istniało szczegółowe uregulowanie prawne (tj. dla każdego badania klinicznego). Wystarczyć może to, że dane uregulowanie prawne stanowi podstawę szeregu operacji przetwarzania w oparciu o obowiązek wykonania zadania realizowanego w interesie publicznym. Zob. również opinia 6/2014 w sprawie pojęcia uzasadnionych interesów administratora danych zawartego w art. 7 dyrektywy 95/46/WE, przyjęta dnia 9 kwietnia 2014 r., WP 217, s. 21–22.

[13] Motyw 50 RODO.

- prawnie uzasadnione interesy administratora zgodnie z art. 6 ust. 1 lit. f) w związku z art. 9 ust. 2 lit. j) RODO;
- w szczególnych okolicznościach, w przypadku spełnienia wszystkich warunków, wyraźna zgoda osoby, której dane dotyczą, zgodnie z art. 6 ust. 1 lit. a) i art. 9 ust. 2 lit. a) RODO.

W imieniu Europejskiej Rady Ochrony Danych

Przewodnicząca

Andrea Jelinek



Opinion 28/2018

regarding the European Commission Draft Implementing Decision

on the adequate protection of personal data in Japan

Adopted on 5 December 2018

Table of contents

1 EXECUTIVE SUMMARY 4
1.1 Areas of convergence 5
1.2 General challenges 5
1.3 Specific commercial aspects 6
1.3.1 Concerns of the EDPB with regards to key data protection principles 6
1.3.2 Need for clarification 7
1.4 On the access by public authorities to data transferred to Japan 7
1.5 Conclusion 7
2 INTRODUCTION 8
2.1 Japan's data protection framework 8
2.2 Scope of the EDPB's assessment 9
2.3 General comments and concerns 10
2.3.1 Specificities of this type of adequacy decision 10
2.3.2 Certainty of translations 10
2.3.3 Sectorial Adequacy 11
2.3.4 Binding nature of Supplementary Rules and of PPC Guidelines 11
2.3.5 Periodic review of the adequacy finding 12
2.3.6 International commitments entered into by Japan 12
2.3.7 Powers of DPAs to bring actions concerning the validity of an adequacy decision before a court 13
3 COMMERCIAL ASPECTS 13
3.1 Content principles 13
3.1.1 Concepts 13
3.1.2 Grounds for lawful and fair processing for legitimate purposes 16
3.1.3 The transparency principle 17
3.1.4 Restrictions on onward transfers 18
3.1.5 Direct marketing 21
3.1.6 Automated decision making and profiling 21
3.2 Procedural and enforcement mechanisms 22
3.2.1 Competent independent Supervisory Authority 22
3.2.2 The data protection system must ensure a good level of compliance 22
3.2.3 The data protection system must provide support and help to individual data subjects in the exercise of their rights and appropriate redress mechanisms 23
4 ON THE ACCESS BY PUBLIC AUTHORITIES TO THE DATA TRANSFERRED TO JAPAN 24

4.1 Law enforcement access to data 25
4.1.1 Procedures for accessing data in the field of criminal law 25
4.1.2 Oversight in the field of criminal law 27
4.1.3 Redress in the field of criminal law 30
4.2 Access for national security purposes 36
4.2.1 Scope of surveillance 36
4.2.2 Voluntary disclosure in case of national security 38
4.2.3 Oversight 38
4.2.4 Redress mechanism 40

The European Data Protection Board

Having regard to Article 70.1(s) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,

Having regard to Article 12 and Article 22 of its Rules of Procedure of 25 May 2018,

HAS ADOPTED THE FOLLOWING OPINION:

1 EXECUTIVE SUMMARY

1. The European Commission endorsed its draft implementing decision on the adequate protection of personal data by Japan pursuant to the General Data Protection Regulation (hereinafter: GDPR)[1] on 5 September 2018[2]. Following this, the European Commission initiated the procedure for its formal adoption.

2. On 25 September 2018, the European Commission asked for the opinion of the European Data Protection Board ("EDPB")[3]. The Commission was requested to provide the EDPB with all the necessary documentation with regards to this country, including any relevant correspondence with the government of Japan.

3. In the light of the discussions held with the EDPB, the European Commission modified twice its draft adequacy decision, and sent its last version on 13 November 2018[4] The EDPB has based its present Opinion on this latest version of the draft implementing decision (hereinafter "draft adequacy decision").

4. The EDPB's assessment of the level of protection ensured by the Commission's adequacy decision has been made on the examination of the decision itself as well as on the basis of an analysis of the documentation made available [5]– by the Commission[6].

5. The EDPB focused on the assessment of both the commercial aspects of the draft adequacy decision and on the government access to personal data transferred from the EU for the purposes of law enforcement and national security, including the legal remedies available to EU individuals. The EDPB also assessed whether the safeguards provided under the Japanese legal framework are in place and effective.

6. The EDPB has used as a main reference for this work its adequacy referential[7] adopted in February 2018.

1.1 Areas of convergence

7. The EDPB's key objective has been to give an opinion to the European Commission on the level of protection afforded to individuals in the Japanese framework. It is important to recognise that the EDPB does not expect the Japanese legal framework to replicate European data protection law.

8. However, the EDPB recalls that to be considered providing an adequate level of protection, the case law of the CJEU as well as Article 45 of the GDPR require that the third country's legislation needs to be aligned to the essence of the fundamental principles enshrined in the GDPR. In the areas of data protection, the EDPB further notes that there are key areas of alignment between the GDPR framework and the Japanese framework on certain core provisions such as data accuracy and minimisation, storage limitation, data security, purpose limitation and an independent supervisory authority, the Personal Information Protection Commission (PPC).

9. In addition to the above, the EDPB welcomes the efforts made by the European Commission and the Japanese authorities to ensure that Japan provides an adequate level of protection to that of the GDPR especially by filling the gaps between the GDPR and the Japanese data protection framework through the adoption of additional rules by the PPC applicable only to personal data transferred from the EU to Japan, the Supplementary Rules. For example, the EDPB notes that the PPC agreed to treat further categories of data as sensitive data (sensitive data under the Japanese legislation do not include sex orientation nor trade union membership). In addition, the Supplementary Rules ensure that data subject rights will apply to all personal data transferred from the EU, irrespective of their retention period (whereas the Japanese legal system provides that data subject rights do not apply to personal data that are set to be deleted within a period of six months).

10. The EDPB also notes the efforts of the European Commission in strengthening the adequacy decision in response to the concerns raised by the EDPB.

1.2 General challenges

11. Nonetheless, challenges remain and the EDPB suggests the following as the main areas that should be strengthened and closely monitored in the Japanese system.

12. The first challenge relates to the monitoring of this new architecture of adequacy, which is combining an existing legal framework with specific Supplementary Rules, to ensure that it will be a sustainable and reliable system that will not raise **practical issues regarding the concrete and efficient compliance** by Japanese entities and enforcement by the PPC.

13. Secondly, the EDPB takes note of the repeated commitments and reassurances of the European Commission and of the Japanese authorities regarding the binding and enforceable nature of the Supplementary Rules whilst inviting the European Commission to **continuously monitor their binding nature and effective application in Japan** as their legal value is an absolutely essential element of the EU – Japan adequacy. With respect to the PPC guidelines, the EDPB would welcome clarifications in

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
[2] See Press release http://europa.eu/rapid/press-release_IP-18-5433_en.htm.
[3] Pursuant to Article 70 (1) (s) of the GDPR.
[4] See Annex I of the EDPB Opinion for the updated version of the draft European Commission implementing decision.
[5] The EDPB based its analysis on translations provided by the Japanese authorities verified by the European Commission
[6] See Annex II of the EDPB Opinion for the list of documents not provided by the European Commission to the EDPB.
[7] WP254, Adequacy Referential, 6 February 2018.

the draft adequacy decision in relation to **their binding nature and asks the Commission to attentively monitor this aspect**[8].

1.3 Specific commercial aspects

14. In the area of the commercial aspects of the draft EU – Japan adequacy decision, the EDPB has some specific concerns and would like to request clarifications on some important matters.

1.3.1 Concerns of the EDPB with regards to key data protection principles

15. The EDPB welcomes that the Supplementary Rules exclude that personal data transferred from the EU is further transferred to a third country on the basis of APEC – CBPRs. In addition, the EDPB recognises that in its new draft of the adequacy decision, the European Commission committed itself to suspend the adequacy decision when onward transfers no longer ensure the continuity of protection.

16. Under the Japanese legislation, one of the legal basis for onward transfers is the recognition of a third country as providing an adequate level of protection to that of Japan. However, the assessment of a third country as adequate by Japan seems not to include the specific "Supplementary Rules" negotiated between the European Commission and the PPC which are only applicable to EU personal data in order to provide for a level of protection essentially equivalent to the GDPR standards. It follows that EU personal data that are transferred from Japan to another third country not recognised as having an essentially equivalent data protection framework to the GDPR on the basis of a Japanese adequacy will not necessarily enjoy the specific protection for EU personal data anymore.

17. **It should however be borne in mind that onward transfers of personal data may occur to third countries which become subject to a possible later Japanese adequacy decision. These third countries may not have been subject of a previous assessment or adequacy finding of the EU. At this point the COM should take over its monitoring role and ensure the level of protection of EU data is maintained or consider suspension of this adequacy decision.**

18. Moreover, the EDPB has concerns in relation to the **consent and transparency obligations** of data controllers (PIHBOs). The EDPB made a careful check of these elements for the reason that, differently to European data protection law, the use of consent as a basis for processing and for transfers has a central role in the Japanese legal system. For example, the EDPB has concerns regarding the notion of consent which is not defined in a way to include the right to withdrawal, an essential element under EU law to ensure the data subject's genuine control over his/her personal data. Regarding the transparency obligations of a PIHBO, there are doubts as to whether proactive information is given to data subjects.

19. The EDPB is concerned that the **Japanese redress system** may not be of easy access to individuals in the EU needing support or wishing to make a complaint in light of the fact that PPC's support is available via Helpline and in Japanese only. The same issue exists with the mediation service provided by the PPC as the system is not publicised on the English version of the PPC's website whilst important informative documents, such as the frequently asked questions on the APPI, are also available in Japanese only. In this respect, the EDPB would welcome if the Commission could discuss with the PPC the possibility of setting up an online service, at least in English, aimed at providing support to, and handle complaints of, individuals in the EU – similar to the one envisaged in Annex II of this adequacy decision. The European Commission will also need to monitor closely the effectiveness of sanctions and of relevant remedies.

[8] See Section 1.3.4 of the present opinion for more information.

1.3.2 Need for clarification

20. The EDPB would welcome assurances on some aspects of the draft adequacy decision on which further clarification is still needed.

21. These relate for example, to some key concepts of the Japanese legislation. More specifically, there is a lack of clarity around the **status of the so-called "trustee"**- a term which resembles to the one of the data processor under the GDPR but whose ability to determine and change the purposes and means of processing of personal data remains ambiguous.

22. The EDPB would also need assurances due to lack of the relevant documents, on whether the **restrictions to the rights of individuals** (in particular, rights of access, rectification, and objection) are necessary and proportionate in a democratic society and respect the essence of fundamental rights.

23. The EDPB would also expect that the European Commission closely monitors the effective protection of **personal data transferred from the EU to Japan, based on the draft adequacy decision, throughout their whole "life cycle"** even though the Japanese legislation imposes a record keeping obligation of the origin of the data for a maximum of three years.

1.4 On the access by public authorities to data transferred to Japan

24. The EDPB has also analysed the legal framework for Japanese governmental entities when accessing personal data transferred from the EU to Japan for law enforcement or national security purposes. While acknowledging the reassurances provided by the Japanese government, referred to as the Annex II to the draft adequacy decision, the EDPB has identified a number of aspects for clarifications and of concern, of which the following should be highlighted.

25. In the area of law enforcement, the EDPB notes that the legal principles applying to access data often appear to be similar to the rules in the EU, to the extent they are available. The lack of available translations of several legal texts and of relevant case law make it difficult, however, to conclude that all the procedures for accessing data are necessary and proportionate and that the application of those principles are applied in a way which is "essentially equivalent" to EU law.

26. In the area of national security, the EDPB recognises that the Japanese government has restated that information may only be obtained from freely accessible sources or through voluntary disclosure by companies, and that it does not collect information on the general public. It is aware, however, of concerns expressed by experts and in the media, and would welcome further clarification on surveillance measures by Japanese governmental entities.

27. As to the legal redress of EU individuals, in the area of law enforcement as well as national security, the EDPB welcomes that the European Commission and the Japanese government have negotiated an additional mechanism for EU individuals to provide them with an additional redress avenue, and thereby extending the powers of the Japanese data protection authority. However, a point of concern remains that this new mechanism does not entirely compensate for the shortcomings of oversight and redress under Japanese law. The EDPB thus seeks for further clarifications in order to ensure that this new mechanism does fully compensate those shortcomings.

1.5 Conclusion

28. The EDPB considers that this adequacy decision is of paramount importance. As the first adequacy decision since the entering into force of GDPR, it will constitute **a precedent for future adequacy**

applications as well as **for the review of the adequacy decisions rendered under Directive 95/46[9].** It is also important to underline that individuals are more and more conscious of the impact of globalisation on their privacy and turn to their supervisory authorities to ensure that adequate guarantees are in place when their personal data are transferred abroad. In light of these implications, the EDPB believes that the European Commission should ensure that there are no shortcomings in the protection offered by the EU-Japan adequacy and that this specific type of adequacy is aligned with the requirements of Article 45 of the GDPR.

29. The EDPB welcomes the efforts made by the European Commission and the Japanese PPC to align as much as possible the Japanese legal framework to the European one. **The improvements** brought in by the Supplementary Rules to bridge some of the differences between the two frameworks are very important and well received.

30. However, following a careful analysis of the Commission's draft adequacy decision as well as of the Japanese data protection framework, the EDPB notices that **a number of concerns, coupled with the need for further clarifications, remain**. Further, this specific type of adequacy combining an existing national framework with additional specific rules also raises questions about its operational implementation. In light of the above, the EDPB recommends the European Commission to address the concerns and requests for clarification raised by the EDPB and provide further evidence and explanations regarding the issues being raised. The EDPB also invites the European Commission to conduct a review of this adequacy finding (at least) every two years and not every four years as suggested in the current draft adequacy decision.

2 INTRODUCTION

2.1 Japan's data protection framework

31. Japan's data protection framework was modernized very recently, in 2017. This framework comprises several pillars, at the centre of which there is a general statutory law, the Act on Protection of Personal Information (APPI). Another important piece of legislation is the Cabinet Order to Enforce the APPI ("Cabinet Order") which specifies certain core principles of the APPI.

32. Based on a Cabinet decision, adopted on 12 June 2018[10] and Article 6 of the APPI, the PPC was given the power to "*take necessary action to bridge the differences of the systems and operations between Japan and the concerned foreign country in view of ensuring appropriate handling of personal information received from each country*"[11]. The Cabinet decision also suggests that the rules adopted by the PPC supplementing or going beyond those laid down in the APPI would be binding and enforceable on the Japanese business operators[12].

33. Accordingly, the PPC engaged in negotiations with the European Commission and adopted, in June 2018, stricter rules to the ones of the APPI and the Cabinet Order to be applied to data transferred from the EU. These are the Supplementary Rules under the Act on the Protection of Personal Information for the Handling of Personal Data Transferred from the EU based on an adequacy decision, hereafter "Supplementary Rules"[13]. These Supplementary Rules are also annexed to the draft implementing Commission decision published in July 2018.

34. It is important to note that the Supplementary Rules are only applicable to personal data transferred from the European Union to Japan on the basis of the adequacy decision and aim at enhancing the applicable protection to those data. As such they do not apply to personal data of individuals in Japan or coming from other countries than the ones of the EEA.

35. Further, the EDPB would like to draw attention to the fact that the amended APPI came into force on May 30, 2017 and the PPC in its current form was established in 2016. Moreover, the Supplementary Rules negotiated by the PPC with the European Commission have yet to enter into force as that will depend on the recognition by the European Commission of Japan as a jurisdiction adequate to the one in the EU.

2.2 Scope of the EDPB's assessment

36. The European Commission's draft adequacy decision is the result of an assessment of the Japanese data protection rules, followed by negotiations with the Japanese authorities. The outcome of these negotiations is notably reflected in the two annexes attached to the draft adequacy decision: the first one provides for additional protections that Japanese business operators will have to apply to the processing of personal data transferred from the EU, while the second one contains assurances and commitments from the Japanese government concerning public authorities' access to data.

37. The EDPB examined the Japanese data protection framework, the Supplementary Rules negotiated by the European Commission and the assurances and commitments from the Japanese government. The EDPB is expected to provide an independent opinion on the European Commission's findings, identify insufficiencies in the adequacy framework, if any, and endeavour to propose alterations or amendments to address these.

38. As mentioned in the EDPB adequacy referential, "*the information provided by the European Commission should be exhaustive and put the EDPB in a position to make an own assessment regarding the level of data protection in the third country*"[14].

39. Nonetheless, the EDPB received most of the documents in English translations, referenced to in the draft adequacy decision, which form an essential part of the Japanese legal system. The EDPB, therefore, renders the present opinion on the basis of the analysis of available documents in English. The EDPB took into account the applicable data protection framework in the European Union, including Article 8 of the European Convention on Human Rights (hereinafter: ECHR) protecting the right to private and family life as well as Articles 7, 8 and 47 of the Charter of Fundamental rights of the European Union (hereinafter: the Charter) respectively protecting the right to private and family life, the right to protection of personal data and the right to an effective remedy and fair trial. In addition to the above, the EDPB considered the requirements of GDPR as well as looking at the relevant jurisprudence.

40. The objective of this exercise is to ensure that the Japanese data protection framework is essentially equivalent to that of the European Union. The concept of "adequate level of protection" which already existed under Directive 95/46, has been further developed by the CJEU. It is important to recall the

[9] Directive No. 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
[10] The EDPB notes that according to the draft adequacy decision this Cabinet Decision was adopted on 12 June 2018. However, the EDPB was only provided with the draft version of the Cabinet Decision, dated April 2018.
[11] Cabinet Decision of April 25th, 2018.
[12] See section 1.3.4 below for more information.
[13] Supplementary Rules, Annex I of the Commission Implementing Decision of XXXX, pursuant to Regulation 2016/679 of the European Parliament and the Council on the adequate protection of personal data by Japan, sent to the EDPB on September 2018.-
[14] WP254, p.3.

standard set by the CJEU in Schrems, namely that – while the "level of protection" in the third country must be "essentially equivalent" to that guaranteed in the EU – "the means to which that third country has recourse, in this connection, for the purpose of such a level of protection may differ from those employed within the [EU]"[15]. Therefore, the objective is not to mirror point by point the European legislation, but to establish the essential and core requirements of the legislation under examination. Adequacy can be achieved through a combination of rights for the data subjects and obligations on those who process data, or who exercise control over such processing and supervision by independent bodies. However, data protection rules are only effective, if they are enforceable and followed in practice. It is therefore necessary to consider not only the content of rules applicable to personal data transferred to a third country or an international organization, but also the system in place to ensure the effectiveness of such rules. Efficient enforcement mechanisms are of paramount importance to the effectiveness of data protection rules[16].

2.3 General comments and concerns

2.3.1 Specificities of this type of adequacy decision

41. The EU-Japan adequacy is the first one to be examined against the new legal backcloth of GDPR. This renders the work of the EDPB all the more important in light of the effects of this draft adequacy decision for future adequacy applications.

42. The EU – Japan adequacy would also be the first mutual one. When and if the EU recognises Japan as providing an essentially equivalent level of protection to the one of the GDPR, Japan will also issue its own adequacy decision under Article 24 of the APPI, recognising the EU as offering an adequate level of protection under the Japanese data protection framework. Thus this envisaged Japan – EU adequacy is of a particular nature which the EDPB has taken into account in its assessment. As mentioned above, the Japanese PPC has negotiated specific, stricter rules with the European Commission, applicable only to personal data transferred from the EU. These stricter rules are binding and enforceable according to the Cabinet Decision and are to be complied with by all Personal Information Handling Business Operators (hereafter PIHBOs) in Japan when processing personal data coming from the EU under this draft adequacy decision.

43. The European Commission has therefore based its adequacy finding not only on the existing general Japanese data protection framework but also on these specific rules. The fact that Supplementary Rules were required to complement the APPI is indicative of the fact that the European Commission acknowledges that the Japanese data protection legislation is not, per se, essentially equivalent to the GDPR.

44. **In light of the above-mentioned issues, the EDPB invites the European Commission to ensure that this new architecture of adequacy, the first to be adopted under the GDPR, relying on Supplementary Rules, will be a sustainable and reliable system that will not raise practical issues regarding the concrete and efficient compliance by Japanese entities and enforcement by the PPC.**

2.3.2 Certainty of translations

45. Like the European Commission, the EDPB has worked on the basis of English translations provided by the Japanese authorities[17]. The EDPB calls the European Commission to clarify that it has based its draft adequacy decision on the English translations received and verify the quality and certainty of these translations regularly.

[15] Case C‑ 362/14, Maximillian Schrems v Data Protection Commissioner, 6 October 2015 (§§ 73, 74).
[16] WP254, p.2.
[17] The European Commission has verified these translations.

2.3.3 Sectorial Adequacy

46. The adequacy finding of this draft adequacy decision is limited to the protection of personal information by PIHBOs within the meaning of the APPI. This means that the adequacy is sectorial as it only applies to the private sector, excluding from its scope transfers of personal data between public authorities and bodies. Currently, the European Commission briefly mentions this specificity of the scope of the adequacy in recital 10 of the draft adequacy decision.

47. **The EDPB invites the European Commission to explicitly mention the sectorial nature of this adequacy finding in the title of the implementing decision as well as in its Article 1 in accordance with Article 45 (3) GDPR.**

2.3.4 Binding nature of Supplementary Rules and of PPC Guidelines

48. Article 6 of the APPI mentions that "the government shall…take necessary legislative and other action so as to be able to take discreet action for protecting personal information that especially requires ensuring the strict implementation of its proper handling in order to seek enhanced protection of an individual's rights and interests, and shall take necessary action in collaboration with the governments in other countries to construct an internationally conformable system concerning personal information through fostering cooperation with an international organization and other international framework." Although the government is clearly identified in this Article of the APPI as competent to take such legal action, it does not refer directly to the PPC as the competent body to adopt specific rules[18]. Due to time constraints, the EDPB was unable to gather, review and examine existing evidence on this point.

49. **In light of the importance of this issue, the EDPB takes note of the repeated commitments and reassurances of the European Commission and of the Japanese authorities regarding the binding and enforceable nature of the Supplementary Rules. The EDPB invites the European Commission to continuously monitor their binding nature and effective application in Japan as their legal value is an essential element of the EU – Japan adequacy.**

50. Moreover, the European Commission makes reference in several sections of its draft adequacy decision to the PPC Guidelines (Guidelines).

51. Although the European Commission clarifies that the Guidelines provide an authoritative interpretation of the APPI in recital 16 of its draft adequacy decision, in the same recital it makes reference to the binding nature of these Guidelines: "According to the information received from the PPC, those Guidelines are considered as binding rules that form an integral part of the legal framework, to be read together with the text of the APPI, the Cabinet Order, the PPC Rules and a set of Q&A prepared by PPC."[19]

52. However, the understanding of the EDPB, based on the same information provided by the PPC, is that the Guidelines are not legally binding. Rather, they provide an 'authoritative interpretation' of the law. The PPC argues that the Guidelines are followed by PIHBOs in practice, used by the PPC for enforcing

[18] According to an article published in July 2018, when the Supplementary Rules were in a draft, the legal binding nature of these Rules was likely to be the object of internal debate in the country. See Fujiwara S., Comparison between the EU and Japan's Data Protection Legal Frameworks', Jurist, vol. 1521 (July 2018): p. 19.
[19] Commission Implementing Decision of XXXX, pursuant to Regulation 2016/679 of the European Parliament and the Council on the adequate protection of personal data by Japan, as sent to the EDPB on November 13, 2018, Recital 16.

the law against PIHBOs and used by courts when rendering their judgment. However, these elements do not constitute sufficient evidence that the Guidelines are legally binding norms.

53. **The EDPB would welcome clarifications in the adequacy decision in relation to the binding nature of the PPC Guidelines and asks the European Commission to attentively monitor this aspect.**

54. According to the PPC, the Guidelines are followed in practice nevertheless as it is local custom. The PPC mentions that the Japanese courts use the PPC Guidelines to render their judgments when applying APPI rules. The European Commission makes reference to a court ruling[20] dating from 2006 to provide evidence that the Japanese courts base themselves on guidelines for their findings. Despite the fact that the EDPB was not provided with this court ruling, the EDPB would appreciate if the European Commission could provide, if available, a more recent court ruling, either in the field of data protection or in another sector where the Japanese courts have used the PPC Guidelines or other similar guidelines as a basis of their decision.

2.3.5 Periodic review of the adequacy finding

55. Article 45 (3) of the GDPR provides that a periodic review must take place at least every four years. According to the EDPB adequacy referential[21], this is a general time frame which must be adjusted to each third country or international organization with an adequacy decision. Depending on the particular circumstances at hand, a shorter review cycle could be warranted. Also, incidents or other information about or changes in the legal framework in the third country or international organization in question might trigger the need for a review ahead of schedule. It also appears to be appropriate to have a first review of an entirely new adequacy decision rather soon and gradually adjust the review cycle depending on the outcome.

56. Taking into account a number of factors, including the fact that the APPI entered into force in 2017, that the PPC was established in 2016 and that there is no information nor evidence on the practical application of the Supplementary Rules yet, **the EDPB invites the European Commission to conduct a review of this adequacy finding (at least) every two years and not every four years as suggested in the current draft adequacy decision.**

2.3.6 International commitments entered into by Japan

57. According to Article 45 (2) (c) of the GDPR and the adequacy referential[22], when assessing the adequacy of the level of protection of a third country, the European Commission shall take into account, among others, the international commitments the third country has entered into, or other obligations arising from the third country's participation in multilateral or regional systems in particular in relation to the protection of personal data, as well as the implementation of such obligations. Furthermore the third country's accession to the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to the Automatic Processing of Personal Data ("Convention 108+"[23] and its Additional Protocol should be taken into account.

58. **In this regard, the EDPB notes that Japan is an observer of the Consultative Committee of Convention 108+.**

[20] Commission Implementing Decision of XXXX, pursuant to Regulation 2016/679 of the European Parliament and the Council on the adequate protection of personal data by Japan, as sent to the EDPB on November 13, 2018, page 5, footnote 16, "Osaka District Court, decision of 19 May 2006, Hanrei Jiho, Vol. 1948, p. 122.
[21] WP254, p.3.
[22] WP254, p.2.
[23] Convention for the protection of individuals with regard to the processing of personal data, Convention 108+, 18 May 2018.

2.3.7 Powers of DPAs[24] to bring actions concerning the validity of an adequacy decision before a court

59. The EDPB underlines that although recital 179 of the draft adequacy decision only mentions cases where a DPA has received a complaint questioning the compatibility of an adequacy decision with the fundamental rights of the individual to privacy and data protection, this statement is to be understood as an example of situations, where a DPA can bring the matter before a national court, which could also be possible in the absence of a complaint, rather than as a restriction to the powers provided to DPAs under the GDPR and national laws of the Member States in this regard. Indeed, the provisions of the GDPR include both the power to suspend data transfers even when based on an adequacy decision and to bring an action concerning the validity of an adequacy decision, are not limited to cases where they have received a complaint, should their national law grant them the power to do so more broadly and independently from a complaint, in accordance with the relevant provisions of the GDPR.

60. **The EDPB invites the European Commission to clarify in its draft adequacy decision that the power of supervisory authorities to bring an action against the validity of an adequacy decision following a complaint is just an illustration of the broader powers of DPAs following from the GDPR, which include the power to suspend transfers and to bring an action concerning the validity of an adequacy decision in the absence of a complaint should their national law provide it.**

3 COMMERCIAL ASPECTS

3.1 Content principles

61. Chapter 3 of the Adequacy Referential is dedicated to the "Content Principles". A third country's or international organisation's system must contain them in order to regard the level of protection provided as essentially equivalent to the one guaranteed by EU legislation. The EDPB acknowledges the fact that the Japanese legal system pursues a different approach to that of the GDPR in order to give effect to the right to privacy. Although the right to privacy is not enshrined in the Japanese Constitution per se, it has been recognised as a constitutional right via case law as also referenced in the European Commission's decision[25].

62. Especially due to the fact that the Japanese approach noticeably differs from the European one, it has to be observed carefully whether, not only single aspects, but the system as a whole ultimately provides an "essentially equivalent" level of protection. This means, that potential "shortcomings" concerning one content principle might be compensated by some other aspects providing adequate checks and balances.

3.1.1 Concepts

63. Based on the adequacy referential, basic data protection concepts and/or principles should exist in the third country's legal framework. Although these do not have to mirror the GDPR terminology, they should reflect and be consistent with the concepts enshrined in the European data protection law. For example, the GDPR includes the following important concepts: "personal data", "processing of personal data", "data controller", "data processor", "recipient" and "sensitive data"[26].

[24] Case C‑ 362/14, Maximillian Schrems v Data Protection Commissioner, 6 October 2015.
[25] The EDPB has not been provided with the English translation of this Court decision. See Commission Implementing Decision of XXXX, pursuant to Regulation 2016/679 of the European Parliament and the Council on the adequate protection of personal data by Japan, as sent to the EDPB on November 13, 2018, footnote 9
[26] WP254, p.4.

64. The APPI also includes a number of definitions such as, among others, those of "personal information", "personal data", "personal information handling business operator". **However, it seems that the APPI does not include a definition of the term "handling of personal data" which is similar to the term "processing of personal data".**

65. Regarding the definition of the term "handling of personal data", the PPC provided written answers to the EDPB's question on this definition. The European Commission quoted this answer to the draft Commission decision "*While the APPI does not use the term "processing", it relies on the equivalent concept of "handling" which, according to the information received by the PPC, covers "any act on personal data" including the acquisition, input, accumulation, organisation, storage, editing/processing, renewal, output, reassure, output, utilization, or provision of personal information.*"[27]

66. However, since the text of reference for this definition has not been provided, the EDPB invites **the European Commission to closely monitor that the definition of the abovementioned concept, as provided by the PPC, is effectively followed in practice.**

3.1.1.1 Concept of data processor and obligations of a "trustee"

67. As mentioned above, the adequacy referential requires that basic data protection concepts and/or principles should exist in the third country's legal framework.

68. The APPI includes a definition of a "personal information handling business operator" which according to the European Commission comprises both the terms of a data controller and a data processor as provided by the GDPR and does not distinguish between the two[28]. However, the APPI also includes a term "trustee" in its Article 22, which in some ways resembles the term of a data processor under the GDPR.

69. As explained by the PPC in its answers provided to the EDPB, and also included in the European Commission's draft adequacy decision, a trustee is considered as the equivalent of a data processor under the GDPR – entrusted with the handling of personal data by a PIHBO. This trustee has the same obligations and rights as any PIHBO, including the ones of the Supplementary Rules for personal data transferred from the EU. The PIHBO that entrusts the handling of personal data to a trustee is bound to "exercise necessary and appropriate supervision"[29] over the trustee.

70. **The EDPB invites the European Commission to explain the trustee's status and obligations when the trustee changes the purposes and means of processing and clarify whether the data subject's consent remains a necessary condition for such change of purpose or determination of means[30].**

[27] Commission Implementing Decision of XXXX, pursuant to Regulation 2016/679 of the European Parliament and the Council on the adequate protection of personal data by Japan, as sent to the EDPB on November 13, 2018, recital 17.
[28] Commission Implementing Decision of XXXX, pursuant to Regulation 2016/679 of the European Parliament and the Council on the adequate protection of personal data by Japan, as sent to the EDPB on November 13, 2018, recital 35.
[29] Article 22 of the Amended Act on the Protection of Personal Information (APPI), put into effect on May 30, 2017.
[30] Art. 23 para 5 (i) APPI. See also section on the transparency principle below.

3.1.1.2 Concept of retained personal data

71. The APPI contains the concept of "retained personal data" which is considered to be a sub-category of personal data. According to the APPI, the provisions relating to the data subject's rights[31]only apply to retained personal data. The definition of retained personal data is included in Article 2(7) of the APPI.

72. Retained personal data are the personal data other than those that (i) are set to be deleted within a period of no longer than 6 months[32] or that (ii) fall under the exceptions of Article 4 of the Cabinet Order and that are likely to harm the public or other interests if their presence or absence is made known.

73. The Supplementary Rule (2) provides that "*personal data received from the EU based on an adequacy decision is required to be handled as retained personal data irrespective of the period within which it is set to be deleted.*"

74. However, personal data falling under the exceptions of Article 4 of the Cabinet Order will not be required to be handled as retained personal data and that data subject rights will not apply.

75. Article 23 of the GDPR provides that, like Article 4 of the Cabinet Order, Union or Member State law to which the data controller/processor is subject to, may restrict the scope of the obligations applicable to him and the rights available to the data subject. This can be done by way of a legislative measure. These restrictions need to respect the essence of the fundamental right and freedoms and is a necessary and proportionate measure in a democratic society.

76. Regarding the substance of the exceptions provided for in Article 4 of the Cabinet Order, the EDPB has not been provided with sufficient documentation on these limitations or additional elements to clarify the scope of these provisions[33]. The EDPB is not in a position to assess whether these limitations to the rights of data subjects are limited to what would be considered strictly necessary and proportionate under EU law, and would thus be essentially equivalent to the rights provided to the EU data subjects.

77. **Due to lack of some relevant documents, the EDPB would also welcome reassurances by the European Commission, if restrictions to the rights of individuals (in particular, rights of access, rectification and objection) are necessary and proportionate in a democratic society and respect the essence of fundamental rights.**

78. An essential requirement under the GDPR is that personal data are protected throughout their whole "life cycle".

79. Taking into account the fact that the Supplementary Rules only apply to personal data transferred from the EU, the EDPB would appreciate receiving further information about the practical implementation of these rules by PIHBOs, especially when these data are further communicated to another PIHBO after their first transmission to Japan.

80. The European Commission has clarified in recital 15 of its draft adequacy decision that PIHBOs receiving and/or further processing personal data from the EU will be under a legal obligation to comply with the Supplementary Rules and that in order to do so they will need to ensure that they can identify such personal data throughout their "life-cycle".

[31] Articles 27-30 of the APPI.
[32] Amendment to the Cabinet Order to Enforce the Act on the Protection of Personal Information (Cabinet Order), put into effect May 30, 2017, Article 5.
[33] The EDPB has not been provided with the Supreme Court decisions referred to in recital 53 of the draft adequacy decision.

81. In its answers, The PPC[34] has explained that such identification will be made by using technical methods (tagging) or organisational methods (storing the data originating from the EU in a dedicated database).

82. In footnote 14 of its draft adequacy decision, the European Commission explains that PIHBOs must record the information on the origin of the EU data for as long as necessary in order to be able to comply with the Supplementary Rules. This is also enshrined in Article 26 (1), (3) and (4) of the APPI which states that a PIHBO is under the obligation to confirm and record the source of these data and all the circumstances surrounding the acquisition of these data.

83. However, the EDPB notes that Article 18 of the PPC Rules[35] specifies that the record keeping obligations of PIHBOs are limited to a maximum of three years for cases that fall outside the specific record keeping methods described in Article 16 of the PPC Rules (using a written document, electromagnetic record or microfilm). This is also stated by the European Commission in recital 71 of its draft adequacy decision: "*As specified in Article 18 of the PPC Rules, those records must be preserved for a period of one to three years, depending on the circumstances*".

84. Even if, as the European Commission states in footnote 14 of its draft adequacy decision, PIHBOs are not prohibited to keep records regarding the origin of the data for longer than three years, in order to be able to fulfil their obligations under Supplementary Rule (2), this is neither clearly reflected in the Japanese legislation nor in the Supplementary Rules. The EDPB considers that there is a risk that PIHBOs will in fact comply with Article 18 of the PPC Rules even when they process data originating from the EU. This is mainly because there is currently, to the understanding of the EDPB and based on available documents, no provision putting PIHBOs under such an obligation to comply with the Supplementary Rules instead. This would result in data transferred from the EU to no longer being protected by the additional protections included in the Supplementary Rules.

85. **The EDPB invites the European Commission to closely monitor the effective protection of personal data transferred from the EU to Japan based on the draft adequacy decision, throughout their whole life-cycle even though the Japanese legislation imposes a record keeping obligation of the origin of the data for a maximum of three years.**

3.1.2 Grounds for lawful and fair processing for legitimate purposes

86. According to the adequacy referential, in line with the GDPR, data must be processed in a lawful, fair and legitimate manner[36]. The legal basis, under which personal data may be lawfully, fairly and legitimately processed, should be set out in a sufficiently clear manner. The European framework acknowledges several such legitimate grounds including, for example, provisions in national law, the consent of the data subject, performance of a contract or legitimate interest of the data controller or of a third party which does not override the interests of the individual.

87. Under the APPI, consent plays a central role in the Japanese data protection legal system. Consent is the central legal basis for the processing of personal data in Japan, and also one of the main legal basis for transfers of personal data from Japan to a third country. In addition, consent is required for an alteration of the purpose of the processing.

88. According to Supplementary Rule (3), the legal basis for the processing of personal data transferred from the EU to Japan will be the legal basis for which the data is transferred to Japan. If the PIHBO wishes to process further these data for a different purpose he needs to obtain the consent of the data subject in advance.

89. The EDPB considers that the quality of consent, especially due to its central role in the Japanese legal framework, has to comply with the fundamental requirements of the notion of consent, i.e. according to EU law, a "*freely given, specific, informed and unambiguous indication of the data subject's wishes*...". The data subject can withdraw such consent as an essential safeguard to ensure the free will of the data subject throughout the time[37]. The right to withdrawal, as a mandatory element of consent, appears to be missing in the Japanese legal framework. Indeed, according to the PPC guidelines[38] the withdrawal is merely "desirable" and conditional to the "characteristics, size and the status of the business activities".

3.1.3 The transparency principle

90. Based on Article 5 of the GDPR, transparency is a fundamental principle of the EU data protection system[39]. The adequacy referential explicitly names "transparency" as one of the content principles to be taken into account when evaluating the essentially equivalent level of protection provided for by a third country. The transparency and fairness principle strives to ensure that the data subject has control over his/her data and, for this purpose, information shall be provided to the data subject in a proactive manner as a rule. In the case of the Privacy Shield, the Article 29 Working Party[40] in their opinion 1/2016 made reference to Annex II, II 1 b of the Privacy Shield agreement (notice to the individual) and stated that, if the data is not collected directly, an organisation should notify the data subject "at the point the data is recorded by the Shield organisation" (section 2.2.1.a). Having the privacy policy publicly available is an additional criterion (see section 2.2.1.b). Hence, already under Directive 95/46/EC it was deemed necessary to directly inform the data subject.

91. A first concern is raised regarding the modality of information provided to the data subject under the APPI. According to Article 27 (1) of the APPI, a PIHBO is obliged to provide the information described in Article 27 (1) APPI by putting it "into a state where a principal can know". However, this wording does not make clear to what extent the PIHBO has to take positive measures to genuinely inform the data subject.

92. **The EDPB invites the Commission to clarify the meaning of the term "can know" and whether the APPI provides as a rule the obligation to genuinely inform data subjects.**

93. Moreover, according to the adequacy referential, restrictions to the information to be provided to the data subject may exist, similar to Article 23 GDPR. On a similar vein, Article 14 (5) of the GDPR provides for an exception to the right to be informed when the information is likely to render impossible or seriously impair the achievement of the processing. However, even in this case, the controller shall provide some sort of information as, for instance, by making "generalised" information publicly

[34] Annex III of the present Opinion.
[35] Enforcement Rules for the Act on the Protection of Personal Information (PPC Rules), put into effect May 30, 2017, Article 16.
[36] WP254, p.4.
[37] GDPR, Article 4(11). For more information see also relevant guidelines of the EDPB on consent WP259, 10 April 2018.
[38] Data Protection Legal and Technical Research and Analysis Consortium (DPC), An assessment of the level of protection of personal data provided under Japanese law, p. 46: "Further, from the viewpoint of protection of rights and interests of a principal such as consumers, it is desirable, in case of having received a demand from a principal for the retained personal data, to further respond to the principal's demand in such a way as stopping etc. of direct-mail sending or voluntarily fulfilling a utilisation cease etc. considering the characteristics, size and the status of the business activities".
[39] WP 254, chapter 3, point 7, p. 5; see also recital (39) GDPR.
[40] This Working Party was set up under Article 29 of Directive 95/46/EC. It was an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC. The WP29 has now become the EDPB.

available. Moreover, when the risk ceases to exist the data subject shall be notified[41]. These aspects are important in order to ensure the fundamental principle of fairness.

94. Under Article 23 of the APPI, a PIHBO generally has to give in advance information to the data subject about providing his/her data to a third party either implicitly when obtaining his/her consent or explicitly by an opt-out notification. The EDPB understands that there is no notification to the data subject, informing him/her of the fact that his/her data are not retained personal data under the APPI because falling under the exceptions of Article 4 of the Cabinet Order. As a result, they will not be able to benefit from their rights in full. The data subjects are not informed in the cases of Article 18(4) APPI either.

95. **The EDPB acknowledges that the rights may be restricted for legitimate objectives pursued by the PIHBO and the state authorities. At the same time, the EDPB considers that there should be at least a general information upfront on the possibility of the restriction of the rights for the objectives referred to the law and that the data subject should be notified when the risks for which the information is restricted cease to exist.**

96. Finally, other aspects of transparency are developed further below. These refer to the risks the transfer to a third country entails[42] and the information on the logic of processing in the context of automated decision making, including profiling.[43]

3.1.4 Restrictions on onward transfers

97. The EDPB welcomes the efforts made by the Japanese authorities and the European Commission to enhance the level of protection for onward transfers in Supplementary Rule (4), which excludes that personal data transferred from the EU is further transferred to a third country on the basis of APEC-CBPRs. In addition, the EDPB recognises that in in recitals 177 and 184 of its new draft of the adequacy decision, the European Commission committed itself to suspend the adequacy decision when onward transfers no longer ensure the continuity of protection. However, the EDPB would like to raise two points regarding these transfers of EU personal data from Japan to third countries.

98. **The use of consent as a basis for data transfers from Japan to a third country in the Japanese legal system raises concerns as the EDPB considers that the information given to the EU data subject prior to consenting seems not to be comprehensive.**

99. Article 24 APPI prohibits the transfer of personal data to a third party outside the territory of Japan without the prior consent of the individual concerned. Supplementary Rule (4) stipulates that EU data subjects have to be provided with information on the circumstances surrounding the transfer necessary to make a decision on his/her consent.

100. The European Commission concludes in its draft adequacy decision that Supplementary Rule (4) secures a particular well informed consent of the EU data subject[44] as he/she will be advised of the fact that the data will be transferred abroad and of the specific country of destination. This would allow the data subject to assess the risk for privacy involved with the transfer.

[41] Tele2, Joined Cases C 203/15 and C 698/15, judgement of the Court, 21 December 2016, rec. 121 and Digital Rights Ireland, Joined Cases C-293/12 and C-594/12, judgement of the Court, 8 April 2014, rec. 54-62.
[42] See section 2.1.4.
[43] See section 2.1.6.
[44] Commission Implementing Decision of XXXX, pursuant to Regulation 2016/679 of the European Parliament and the Council on the adequate protection of personal data by Japan, as sent to the EDPB on November 13, Recital 76.

101. Under the transparency principle of the adequacy referential, a certain degree of fairness shall be ensured when informing individuals. In the context of onward transfers based on consent, the EDPB is of the opinion that to ensure such adequate degree of fairness data subjects should be explicitly informed about the possible risks of such transfers arising from the absence of adequate protection in the third country and the absence of appropriate safeguards prior to consent. Such notice should include for example information that in the third country there might not be a supervisory authority and/or data processing principles and/or data subject rights might not be provided for in the third country[45]. For the EDPB the provision of this information is essential in order to enable the data subject to consent with full knowledge of these specific facts of the transfer[46].

102. Informed consent is also important regarding sectorial exclusions. The adequacy decision does not cover certain types of processing by certain bodies such as universities for the processing of personal data for academic purposes. The EDPB's concern here relates to the specific scenario of when data transferred from the EU under the adequacy decision – for example the HR data of Erasmus students in Japan – are then used for a different purpose falling out of the scope of the adequacy decision (e.g. research purposes), with the consent of the data subject, - and are therefore no longer covered by the additional protection provided by the Supplementary Rules.

103. The European Commission states in recital 38 of its draft adequacy decision that such a scenario will fall under the context of onward transfers and that, where this takes place, the PIHBO has to provide the data subject with all the necessary information before obtaining his/her consent, including that the personal information would not fall under the protection of the APPI rules.

104. Supplementary Rule (4) only requires the PIHBO to obtain the data subject's consent after having been provided with information on the circumstances surrounding the transfer necessary for the principal to make a decision on his/her consent.

105. **The EDPB invites the European Commission to ensure that the information to be provided to the data subject "on the circumstances surrounding the transfer" should include the information about the possible risks of transfers arising from the absence of adequate protection in the third country and the absence of appropriate safeguards, or in the case of sectorial exclusions, of the absence of protections of the Supplementary Rules and of the APPI.**

106. **Onward transfers of personal data may occur to third countries, which become subject to a possible later Japanese adequacy decision.**

107. Without prejudice to the derogations set forth in Article 23 para 1 of the APPI, data initially transferred from the EU to Japan can be then transferred from Japan to a third country without consent in two cases:

- If the PIHBO and the third party recipient have together implemented measures providing a level of protection equivalent to the APPI read together with the Supplementary Rules by means of a contract, other forms of binding agreements or binding agreements within a corporate group[47].

[45] EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, 25 May 2018, p.8.
[46] EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, 25 May 2018, p.7.
[47] Supplementary Rule (4) (ii).

- If the third country has been recognised by the PPC under Article 24 of the APPI and Article 11 of the PPC Rules[48] as providing an equivalent level of protection to the one guaranteed in Japan.

108. The EDPB evaluates Article 24 APPI as the more specific rule, which contains a derogation from the general rule under Article 23 APPI. Therefore, the EDPB does not share the European Commission's assessment in the new last sentence of Recital 78 of the draft adequacy decision stating that even in those cases, the transfer to the third party remains subject to the requirement to obtain consent under Article 23 (1) of the APPI.

109. Pursuant to Article 11 (1) of the PPC Rules, an adequacy decision by the PPC requires substantive standards equivalent to the APPI whose implementation are ensured in the third country and which are effectively supervised by an independent enforcement authority. Moreover, the PPC may impose necessary conditions to protect the rights and interests of individuals in Japan, according to Article 11 (2) of the PPC Rules.

110. Supplementary Rule (4) states that EU personal data can be transferred to a third country subject to a Japanese adequacy decision without further restrictions. But Article 44 of the GDPR regulates that any transfer of personal data to a third country has to fulfil the conditions laid down in Chapter V of the GDPR including onward transfers from the third country to another third country. The level of protection of natural persons whose data is transferred must not be undermined by the onward transfer[49]. Although this interpretation is in principle also shared by the European Commission in its draft adequacy decision[50], it seems not to be completely followed. The European Commission has negotiated the prohibition of data originating from the EU being transferred to a third country on the basis of Asia Pacific Economic Cooperation (APEC) – Cross Border Privacy Rules (CBPRs). In the light of the comparative tool developed in 2014 under the framework of the EU Directive between BCR and CBPR showing the requirements of both systems, their convergences and differences (WP29 Opinion 02/2014), the EDPB has concerns about the use of CBPRs as an onward transfer tool for personal data transferred from the EU to countries outside of Japan.

111. In contrast, onward transfers of personal data transferred from the EU to Japan on the basis of a Japanese adequacy decision, seem to be accepted by the European Commission, without the possibility for the PPC to impose the Supplementary Rules as conditions to protect the rights and interests of EU individuals, if necessary. The EDPB deduces from Article 44 of the GDPR that the enhanced protection of data being transferred from the EU to Japan foreseen in the Supplementary Rules has always to be extended when personal data transferred from the EU to Japan is further transferred to a third country, if the data protection framework in that country is not recognised as essentially equivalent to the GDPR.

112. **Hence, the EDPB invites the European Commission to take over its monitoring role and to ensure the level of protection of EU data is maintained or to consider suspension of this adequacy decision if personal data transferred from the EU to Japan is further transferred to third countries subject to a possible later Japanese adequacy decision, when these third countries have not been subject of a previous assessment or adequacy finding of the EU.**

[48] Enforcement Rules for the Act on the Protection of Personal Information, 30 May 2017. An English translation of the new Article 11 was communicated by the EU Commission to the EDPB, but this Article has not been published yet.

[49] WP 254, p.5.

[50] Commission Implementing Decision of XXXX, pursuant to Regulation 2016/679 of the European Parliament and the Council on the adequate protection of personal data by Japan, as sent to the EDPB on November 13, Recital 75.

3.1.5 Direct marketing

113. According to Supplementary Rule (3), a PIHBO is prohibited from processing the data for the purpose of direct marketing if it has been transferred from the European Union for another purpose and the EU data subject has not given his or her consent to the change of the utilisation purpose.

114. According to the Adequacy referential where data are processed for the purposes of direct marketing, the data subject should be able to object without any charge from having his/her data processed for such purposes at any time. According to Article 16 of the APPI, a PIHBO is only allowed to process personal information if the data subject gives his or her consent. The withdrawal of consent could provide the same result as the privileged right to object to direct marketing.

115. The Japanese data protection framework does not provide a privileged right of objection and as explained above in the section on consent, withdrawal of consent under the PPC Guidelines is merely desirable and conditional and can therefore not be considered to equate to a right to object at any time as requested under the Adequacy referential. **The EDPB invites the European Commission to provide reassurances about the right to withdrawal of consent and to monitor cases regarding direct marketing.**

3.1.6 Automated decision making and profiling

116. According to the adequacy referential, decisions based solely on automated processing (automated individual decision-making), including profiling, which produce legal effects or significantly affect the data subject, can take place only under certain conditions established in the third country legal framework. Therefore, every time automated decision making and profiling under the aforementioned circumstances is conducted, there has to be a legal ground for this.

117. In the European framework, the conditions for automated decision making include, for example, the need to obtain the explicit consent[51] of the data subject or the necessity of such a decision for the conclusion of a contract. If the decision does not comply with such conditions as laid down in the third country legal framework, the data subject should have the right not to be subject to it. Furthermore, the law of the third country should, in any case, provide for necessary safeguards, including the right to be informed about the specific reasons underlying the decision and the logic involved to correct inaccurate or incomplete information and to contest the decision where it has been adopted on an incorrect factual basis.

118. The Commission decision only refers to banking sector where sectoral rules[52] regarding automated decisions would apply. The Comprehensive Guidelines for Supervision over Major Banks mentioned in recital 93 of the draft adequacy decision indicate that the concerned individual has to be provided with specific explanations on the reasons for the rejection of a request to conclude a loan agreement.

119. The argumentations of the European Commission referring to the draft adequacy decision (Recital 94), that the absence of specific rules on automated decision making in the APPI is unlikely to affect the level of protection seems (for instance) do not to take into account the case in which an EU-transferred

[51] For critical remarks to the concept of consent in the Japanese data protection legal framework see: 2.1. General and 2.2.8. Direct marketing.

[52] These Sectoral Rules were not provided to the EDPB.

personal data is subsequently processed by another Japanese data controller (different from the original Japanese data importer).

120. It appears therefore, that there are no general rules applicable across sectors in Japan governing automated decision making and profiling.

121. **The EDPB invites the European Commission to monitor cases related to automated decision making and profiling.**

3.2 Procedural and enforcement mechanisms

122. Based on the criteria set in the adequacy referential, the EDPB has analysed the following aspects of the Japanese data protection and legal framework as covered under the draft adequacy decision: the existence and effective functioning of an independent supervisory authority; the existence of a system ensuring a good level of compliance and a system of access to appropriate redress mechanisms equipping EU individuals with the means to exercise their rights and seek redress without encountering cumbersome barriers to administrative and judicial redress.

123. Building on the parameters established by the CJEU in the Schrems case[53] and those outlined in recital 104 and Article 45 of the GDPR, the EDPB finds that, although a system consistent with the European one exists in Japan, this system may be difficult to access in practice for EU individuals, whose data will be transferred under this adequacy decision in light of the existence of language and institutional barriers.

124. The sections below will examine the above mentioned aspects of the Japanese framework before highlighting some recommendations for the Commission.

3.2.1 Competent independent Supervisory Authority

125. The PPC was established on the 1 January 2016 following the amendments of the APPI of 2015, replacing its predecessor – the Specific Personal Information Protection Commission (established in 2013 under the My Number Act). Although a young organization, since its establishment, the PPC has put considerable efforts into building the required infrastructure to accommodate the implementation of the amended APPI. Noticeable among these are the establishment of the PPC's rules, the PPC Guidelines to give guidance to PIHBOs on the interpretation of the APPI, the publication of a PPC Q&A[54] document and the setting up of a helpline to advise business operators and citizens on data protection provisions as well as of a mediation service to handle complaints.

126. The establishment and functioning of the PPC is regulated in chapter V of the APPI. Although the PPC falls within the jurisdiction of the Prime Minister, article 62 mandates that the PPC exercises its function independently. The EDPB welcomes the clarification made by the European Commission in the amended draft of the adequacy decision circulated on 13 November 2018 to further describe the degree to which the PPC is free from internal and external influences.

3.2.2 The data protection system must ensure a good level of compliance

127. The draft adequacy decision undertakes a comprehensive examination of the powers that the PPC is equipped with under Articles 40, 41 and 42 of the APPI to ensure the monitoring and enforcement of the legislation. Article 40 empowers the PPC to request PIHBOs to submit reports and documentation relating to processing operations as well as to carry out on-site inspections. Under Article 42, the PPC has the power – when recognising that it is necessary to protect individual rights or where finding a violation of the provisions of the law – to issue recommendations and, those failing, orders to PIHBOs to suspend the act of violation or take necessary measures to rectify the violation.

128. In October 2018, the PPC took one of its first actions under article 41 of the amended APPI and issued 'guidance' to a PIHBO, advising the company to strengthen its' security measures and to effectively supervise applications providers whilst giving clear and easy to understand explanations to users on how their personal information is used, and obtain consent beforehand when the information is shared with a third party as well as respond properly to users' request for erasure of their information. In the answers provided to the EDPB[55], PPC officials advised that the company has announced it will cooperate and that, when the company fail to do so, it will render the company with a 'recommendation' under Article 42(1) of the APPI.

129. The investigation conducted by the PPC on the above mentioned PIHBO is a very positive indicator of the Japanese supervisory authority's efforts to ensure a good level of compliance in the country.

130. Although there are improvements in respect to the framework in place prior to the 2015 amendments, the EDPB notices that the PPC has fewer powers than European DPA under the GDPR, especially in relation to **enforcement**. Administrative fines[56], for example, are quite mild. The European Commission's decision emphasises in recital 108 that, in cases of non-compliance or some violations of the APPI, criminal sanctions are in place and that the PPC Chair may forward cases to the public prosecutor. However, the European Commission's decision does not account for the fact that public prosecution in Japan is discretional and may sometimes be subject to lengthy review processes[57]. In addition, the penalty of imprisonment (with or without labour) associated with violations of the APPI pursuant the provisions in Chapter VII may be difficult to execute because directed at natural persons and, in any case, not punishing the PIHBO as a legal entity failing to exercise its accountability obligations.

131. **In light of the above, the EDPB invites the European Commission to closely monitor the effectiveness of sanctions and relevant remedies in the Japanese data protection system.**

3.2.3 The data protection system must provide support and help to individual data subjects in the exercise of their rights and appropriate redress mechanisms

132. The PPC provides extensive information and guidelines on its website aimed at raising awareness among PIHBOs in relation to their obligations and responsibilities under the data protection framework as well as a Helpline to provide information and support to Japanese citizens regarding their individual rights under the APPI. The website has also a section, called the 'Children's room', explicitly aimed at a children's and young people audience. The EDPB observes that this information – along with the Helpline support, guidance and Q&A documentations – is available in Japanese[58]. Therefore, the EDPB strongly believes, it would be beneficial if the PPC could provide a dedicated page on the English version of its website aimed at providing information about their individual rights under the Japanese

[53] Case 362/14 (2015) Maximilian Schrems v Data Protection Commissioner, (para. 73 and 74).
[54] This document was not provided by the European Commission to the EDPB in English.

[55] Annex III.
[56] These are provided in Chapter VII of the APPI. The maximum penalty is provided by art. 83 (provision or use by stealth of a personal information database for own or a third party's illegal profit) and is equivalent to either a year's imprisonment with work or a fine not exceeding 500,000 yen (roughly EUR 3900). According to the explanations provided by the Commission, fines are cumulative per infringement. Although this may be the case, the EDPB observes that, even if cumulative fines are applied, the total amount is likely to remain considerably low compared to European standards.
[57] Oda H., Japanese Law, Oxford University Press (III edition), 2009: 439 – 440.
[58] https://www.ppc.go.jp/en/contactus/piinquiry/.

data protection framework and under the Supplementary Rules to EU individuals whose data will be transferred to Japan under the European Commission's adequacy decision.

133. The EDPB welcomes the clarification made by the European Commission in recital 104 of the amended draft adequacy decision circulated on 13 November 2018 regarding the mediation service managed by the PPC pursuant Article 61(ii) of the APPI. However, the EDPB would like to raise three points in relation to this. Firstly, the mediation service is not publicized on the English version of the PPC's website. Secondly, the service is accessible only via phone and available in Japanese. Finally, mediation is merely a facilitative process not leading to a binding agreement between the parties which has implications for the effectiveness of the redress options available to data subjects[59].

134. Finally, the EDPB notices that the draft adequacy decision places emphasis on the remedies available through civil law action as well as criminal proceedings, but does not acknowledge the existence of **institutional barriers to litigation** in Japan such as legal costs (legal fees are split equally between plaintiff and defendant, regardless of which party wins the proceedings[60]), dearth of lawyers in the country[61], the fact that foreign lawyers are not allowed to practice domestic law as well as the burden of proof requirement under Tort Law. The EDPB fears that these factors may – in practice – hinder individuals' access to justice and jeopardise their right to pursue legal remedies rapidly and without bearing prohibitive costs.

135. In light of the above, **the EDPB is concerned that there is a risk that EU individuals may have difficulties accessing administrative and judicial redress** and, therefore, would welcome if the European Commission could discuss with the PPC the possibility of setting up an online service, at least in English, **aimed at providing support to, and handle complaints of[62], EU individuals**. In addition, the EDPB would welcome the possibility of allowing EU DPAs to act as intermediaries for EU data subject complaints with organisations operating in Japan and the PPC.

4 ON THE ACCESS BY PUBLIC AUTHORITIES TO THE DATA TRANSFERRED TO JAPAN

136. The intention of the COM is to recognise, through the adequacy decision, that "Japan ensures an adequate level of protection for personal data transferred from the European Union to personal information handling business operators in Japan", as stated in Art. 1 of the draft adequacy decision. In line with Art. 45 (2) GDPR, the COM has also analysed the limitations and safeguards as regards access to personal data by public authorities. This chapter focuses on the assessment of the access to personal data by law enforcement authorities and by other government entities for the purpose of national security. The analysis of the EDPB is based on the draft adequacy decision, its Annex II, in which the Japanese government provides an overview of the relevant legal framework, and the Japanese legal texts, to the extent they were provided by the COM. Therefore, in the specific context of this assessment, the EDPB has taken into account elements concerning Japanese laws which are not part of the findings by the European Commission, but that are relevant to assess the conditions and safeguards under which Japanese public authorities are allowed to access personal data transferred from the European Union.

4.1 Law enforcement access to data

4.1.1 Procedures for accessing data in the field of criminal law

137. The draft adequacy decision presents three ways foreseen under Japanese law for law enforcement authorities to access data in Japan:

4.1.1.1 Access requests with a court warrant

138. The draft adequacy decision states that for government access in Japan, and especially for criminal law enforcement authorities to request access to electronic evidence in the context of criminal investigations, they always need to have a warrant, unless they use the voluntary disclosure procedure – see below.

4.1.1.1.1 Requirement of "adequate cause", necessity and proportionality of the warrants

139. The EDPB acknowledges that under the Japanese constitution any collection of personal data by compulsory means must be based on a court warrant. More specifically, the draft adequacy decision indicates that in all cases of "searches and seizures", court warrants have to be issued for "adequate cause", which the Supreme Court considers only exists where the individual concerned (suspect or accused) is considered to have committed an offence and the search and seizure is necessary for the criminal investigation. The COM here references the Supreme Court judgment of 18 March 1969, case N. 100 (1968(Shi)).). The EDPB recalls that under the CJEU's case law[63] only a court, and not prosecutors for instance, can authorize the collection of traffic and location data in particular.

140. Also in light of the CJEU jurisprudence, according to which access to data may be subject to a warrant, as in Tele2, the EDPB regrets that no additional information were provided in order to assess how the criteria for assessing the necessity of a warrant – gravity of the offense and how it was committed ; value and importance of the seized materials as evidence ; probability of concealment or destruction of seized materials ; extent of the disadvantages caused by a seizure ; other related conditions – and the concept of "adequate cause" derived from the Constitution are applied in practice. Therefore, the EDPB invites the Commission to monitor if the issuing of warrants meets the criteria set out by the CJEU in practice.

4.1.1.1.2 Types of crimes for which warrants can be issued

141. The warrant procedure applies only whenever a "compulsory investigation" is carried out. In principle, these warrants can only be issued in cases where a violation of law has occurred. In this respect, the EDPB notes the recently adopted "Act on Punishment of Organized Crimes and Control of Crime Proceeds" on 15 June 2017 in the context of adherence of Japan to the UN international Convention on Transnational Crime (UNTOC)[64]. In the absence of an English available version of this legislation, and given the requirement under EU law that some data are collected only in the context of investigation, detection or prosecution of serious crimes[65], as well as given concerns expressed by several commentators, including UN Special Rapporteur Joseph Cannataci[66], concerning the wide scope of application, and which relies on a definition of "organized criminal group" reportedly vague

[59] Kojima T., *Civil Procedure and ADR in Japan*, Chuo University Press, 2004; and Menkel-Meadow C., *Dispute Processing and Conflict Resolution: Theory, Practice and Policy*, Ashgate (2003) (ed.).
[60] Wagatsuma (2012), 'Recent Issues of Cost and Fee Allocation in Japanese Civil Procedure' in Reimann (ed.), Cost and Fee Allocation in Civil Procedure – Ius Gentium; comparative Perspectives on Law and Justice Vol. 11, pp. 195 – 200.
[61] According to the latest figures, the number of lawyers in Japan is 38,980 (roughly 290 layers per one million people [Japan Federation of Bar Association] (2017), White Paper on Attorneys: p. 8 – 9.
[62] Similar to the one envisaged in Annex II of this adequacy decision for complaints from EU residents regarding access to their data by Japanese public authorities.
[63] See cases 203/15 and C 293/12 and C 594/12 of the CJEU.
[64] See: https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html .
[65] See joint cases C 293/12 and C 594/12 and case C 203/15.
[66] UN Special rapporteur on the right to privacy, as well as Graham Greenleaf, UNSW Law Researcher.

and too broad, the EDPB is not in a position to conclude that access to electronic evidence under the relevant Japanese legislation is limited to the thresholds provided by EU law.

142. It has also to be noted that for some types of offences, the Prefectural Police is competent and that they have their specific police ordinances. The internal rules applicable to the Prefectural police were not available to the EDPB.

143. According to the draft Adequacy decision, the collection of electronic information in the area of criminal law enforcement falls under the responsibility of the Prefectural Police.

4.1.1.2 Wiretapping warrants

144. Annex II of the draft adequacy indicates that the Act on Wiretapping for Criminal Investigation provides for specificities for the interception of communications. This legislation was provided very late which did not allow for an in-depth analysis. Therefore, although many safeguards seem to be provided within this legal framework, the EDPB is not in a position to assess whether the conditions provided in this piece of legislation are surrounded by guarantees substantially equivalent to those required in the EU both by the Charter as interpreted by the CJEU and by the ECHR as interpreted by the Strasbourg Court.

4.1.1.3 The "voluntary disclosure" procedure based on enquiry sheet

145. This non-compulsory form of cooperation allows public authorities to ask controllers (except telecommunications carriers) to provide them with data they have. Non-compliance with the request cannot be enforced. It remains unclear which authorities can use this type of procedure, but it appears limited to those investigating crimes.

4.1.1.3.1 Conditions to issue "enquiry sheets"

146. The EDPB acknowledges that the Japanese Supreme Court, by reference to the Constitution, has framed limitations to the use "voluntary disclosures"[67]. It appears from the draft adequacy decision that concretely a "voluntary disclosure" may only be asked by the competent authorities through the issuance of an "enquiry sheet". Sending such an "enquiry sheet" is said to be permissible only as part of a criminal investigation, and thus to always presuppose a concrete suspicion of an already committed crime. Such investigations are generally carried out by the Prefectural Police, where the limitations pursuant to Article 2(2) of the Police Law apply, which means it should be relevant for the Police activities. However, the EDPB seeks further clarification as to the concrete contours of the criteria allowing to issue an enquiry sheet (such as case law illustrating the application of these criteria), and the relationship between the voluntary disclosure procedure and the seizure of data on the basis of a warrant. Indeed, it appears that even where data could not be obtained through the voluntary procedure, they could still be obtained with a warrant if indispensable for the investigative authorities[68].

4.1.1.3.2 Available case law on the limitations to the use of voluntary disclosure

147. The cases quoted in the draft adequacy decision[69] to illustrate limitations to the use of voluntary disclosure procedures relate to cases, where the accused person was either photographed or filmed in the public space by the police directly, and therefore give limited indications as to situations where the competent authorities can ask a controller to disclose data, in particular with regards to the criteria listed under Annex II concerning the "appropriateness of methods", which seems to concern the

[67] See Annex II page 8.
[68] See Annex II page 7.
[69] See Annex II page 8 – two Supreme Court decisions of December 24th, 1969 (1965 (A) No.1187) and April 15th, 2008 (2007 (A) No.839).

assessment of whether voluntary investigation is "appropriate" or reasonable in order to achieve the purpose of the investigation. The same can be said concerning the general criteria of "whether it can be considered reasonable in accordance with socially accepted conventions" to assess the legality of voluntary investigations. Furthermore, the National Police Agency, which is the federal authority in charge of all matters concerning the criminal police, issued instructions to the Prefectural Police on the "proper use if written inquiries in investigative matters". Among others, the chief investigator must receive internal approval from a high-ranking official. The EDPB has no information if these instructions are binding. Nevertheless the EDPB states, that the use of this procedure has to be proportionate or necessary.

4.1.1.3.3 Rights and obligations of the controllers in the context of voluntary disclosure

148. In addition, it is for the controllers to consent to provide data (but there appears to be no obligation on their part to seek the consent of data subjects or to inform them), where these requests do not conflict with other legal obligations (such as confidentiality obligations). The report provided by the Commission seems to indicate that after a high rate of compliance, controllers have started taking into account data protection of their customers' and thus have started answering less frequently to these requests.

149. It also remains unclear if controllers have any incentive to comply with the requests (for instance, if they have an advantage when complying, or if they are exempted from prosecution, etc). In particular, no mention is made of any principle such as the "non-self-incrimination principle".

150. The EDPB would welcome additional information, if available, figures on the number and types of requests, as well as on the answers provided by the controllers requested. In the absence of case law and figures, the EDPB invites the Commission to monitor the efficiency and concrete application of this procedure in practice

151. However, the EDPB lacks case law and figures on this procedure to establish these elements. Consequently, the EDPB is not in a position to provide an assessment concerning the efficiency and concrete application of this procedure without further elements concerning the practice.

4.1.1.4 Conclusion on procedures for accessing data for law enforcement purposes

152. As a conclusion, the EDPB acknowledges that the principle according to which personal data can be compulsorily accessed by the competent authorities only when necessary and proportionate to the purpose, and on the basis of a warrant, corresponds to the main essential guarantees provided under EU and ECHR law. Following the findings above, the EDPB asks the Commission to monitor the scope of these measures, the scope of the voluntary disclosure procedure and the application of these principle by the Prefectural Police and by the Courts in the relevant case law and to monitor too, if the Japanese legal framework is providing the essential guarantees drawn by the CJEU on the basis of the Charter and the ECHR on the basis of the Convention.

4.1.2 Oversight in the field of criminal law

153. The draft adequacy decision as well as the Annex II present four types of oversights conducted on the police, ministries and public agencies.

4.1.2.1 Judicial oversight

4.1.2.1.1 In cases where electronic information is collected by compulsory means (search and seizure)

154. According to the draft adequacy decision, in all cases where electronic information is collected by compulsory means (search and seizure), the police has to obtain a prior court warrant. However, there

is an exception to this rule. [70]. Indeed, article 220 (1) of the Code of Criminal Procedure allows a public prosecutor, its assistant or a judicial police official, when they are arresting a suspect to search or seize electronic information on the spot of the arrest. In this situation, there is a possibility for those information to be excluded as evidence by a judge.

155. The EDPB is mindful that similar exceptions also exist under EU law. It notes that there is not always a judicial control in cases where electronic information is collected by compulsory means, as it is stipulated in the draft adequacy decision. In this context, the EDPB recalls the jurisprudence of the ECHR on judicial a posteriori checks.[71]

4.1.2.1.2 In the case of requests for voluntary disclosure

156. According to the draft adequacy decision, in the case of the requests for voluntary disclosure, there is no ex ante control by a judge. In such case, the Prefectural Police operates under the supervision of the public prosecutor. The draft adequacy decision mentions articles 192 (1) and 246 on the mutual cooperation and coordination of the prosecutors, Prefectural Public Safety Commission and Judicial Police Officials and exchange of information between them. It also refers to article 193 (1) according to which public prosecutor may give necessary instruction to judicial police as well as setting standards for fair investigation. Finally, it mentions article 194 on the disciplinary actions against judicial police for not respecting the public prosecutors taken by the National or Prefectural Public Safety Commission.

157. The EDPB acknowledges the establishment of the previous measures and the oversight conducted by National and Prefectural Public Safety Commission on the judicial police (see below).

4.1.2.2 Oversight by the Public Safety Commissions of the police

158. According to the Annex II of the draft adequacy decision, two types of commissions are exerting an oversight of the police. Both aim at securing democratic management and political neutrality of the police administration.

4.1.2.2.1 Oversight conducted by the National Public Safety Commission

159. Annex II of the draft adequacy decision mentioned the oversight conducted by the National Public Safety Commission on the NPA. The Police Law gives a list of the duties of the Commission from which emanates its supervisory powers (see Article 5).

160. According to Article 4 of the Police Law, the National Public Safety Commission is established under the jurisdiction of the Prime Minister and is composed of a chairman and five members. Article 7 establishes some limitations to the appointment of the members of the Commission. The term of Office of Members of the Commission is five years and may be re-conducted one time only, as prescribed in Article 8. Furthermore, the Diet, appears to have a strong power over the appointment and the dismissal of the Commission's member which ensure the independence of the National Public Safety Commission.

161. Such legal provisions enhance the political neutrality of the National Public Safety Commission.

4.1.2.2.2 Oversight conducted by Prefectural Public Safety Commissions

162. The Prefectural Police is subject to the oversight of the Prefectural Public Safety Commissions established in each prefecture. According to Articles 2 and 36 (2) of the Police Law, the Prefectural Public Safety Commissions are responsible for "the protection of rights and freedom of an individual". Article 38 as well as Article 42 of the Police Law list the duties of the Prefectural Public Safety Commissions. Those Commissions also aim at securing democratic management and political neutrality of the police administration as stated in Article 43 (2) by issuing to the Prefectural Police individual cases when they consider this necessary in the context of an inspection of the activities of the Prefectural Police or misconduct of its personnel.

163. However, it is unclear whether those Commissions have other powers than the inspection of police's behavior. The EDPB is wondering whether the term "misconduct" is including illegal access of data and, in such a case, whether those Commissions are able to order the deletion of data or not.

164. Regarding the neutrality and the independence of those Commissions, as stated in the draft adequacy decision[72], Prefectural Public Safety Commissions are established under the jurisdiction of the prefectural governor who has to appoint members of the Commission with the consent of the prefectural assembly. Members of the Prefectural Public Safety Commission have a three years term and may be re-appointed up to two times. Article 39 of the Police Law enounced limitations concerning the appointment of the members. The draft adequacy decision also mentions the oversight of the Prefectural Police by local assembly, making reference of Article 100 of the Local Autonomy Act. However, this act was not provided to the EDPB[73].

165. Furthermore, according to Article 42 (2) and (3) of the Police Law, "No member of the Commission shall become concurrently a member of the assembly or the personnel in full-time service of local public entities or be engaged in part-time service prescribed in the provision of paragraph 1, Article 28 (5) of the Local Public Service Law.

166. According to the elements stated above and considering the collaboration between Prefectural Public Safety Commissions and National Public Safety Commission, the EDPB agrees with the draft adequacy decision and welcomes the neutrality and the independence of the members of the Prefectural Public Safety Commissions. The EDPB understands that Prefectural Safety Commissions only have a power to investigate police's behavior and do not have other supervisory powers, including the deletion of data collected by the prefectural police. Therefore, it appears that further clarification is needed as to whether the oversight conducted by Prefectural Public Safety Commissions is sufficient according the standards established under EU law.

4.1.2.2.3 Oversight conducted by the Diet

167. The draft adequacy decision[74] and the Annex II[75] are providing some information about the oversight conducted by the Diet in relation to the government, including with respect to the lawfulness of information collection of data by the police. Indeed, both mention the Article 62 of the Constitution according to which, the Diet may request the production of documents and the testimony of witnesses. Both are also mentioning legal provisions from the Diet Law, especially Article 104, concerning the powers of the Diet as well as Article 74 on the submission of written inquiries, which have to be answered by the Cabinet in writing within seven days as prescribed in Article 75. The draft adequacy decision also adds "The Diet's role in supervising the executive is supported by reporting obligations, for instance pursuant to Article 29 of the Wiretapping Act".

168. The EDPB acknowledges the implication of the Diet in the oversight of the government and the police regarding the lawfulness of data collection.

[70] See Annex II.
[71] ECHR, Modestou v. Greece, N° 51693/13.
[72] See draft adequacy decision p. 31.
[73] See draft adequacy decision p. 33.
[74] See draft adequacy decision p. 30.
[75] See Annex II, p. 12.

4.1.2.2.4 Oversight conducted by the executive

169. According to the Annex II of the draft adequacy, on the one hand, the Minister or Head of each ministry or agency has the authority of oversight and enforcement based on the APPIHAO[76]. On the other hand, the Minister of Internal Affairs and Communications (MIC) has an investigative power concerning the enforcement of the APPIHAO by all other ministries, including the Minister of Justice for the Police as mentioned in the draft adequacy decision[77].

170. The Minister may request the head of an administrative organ to submit materials and explanations regarding the handling of personal information by the concerned administrative organ based on Article 50 of the APPIHAO. It may request a revision of the measures when it is suspected that a violation or inappropriate operation of the Act has occurred as well as issuing opinions concerning the handling of personal information by the concerned Administrative Organ according to Articles 50 and 51 of the APPIHAO.

171. The draft adequacy decision and the Annex II are also mentioning the establishment of 51 comprehensive information centres which are "ensuring the smooth implementation of this Act" according to Article 47 of the APPIHAO. The EDPB notes that the APPIHAO does not explain further the role and powers of those information centres but the draft adequacy decision provides some precisions.

172. Therefore, the EDPB welcomes the fact that there is an executive oversight on the respect of the APPIHAO on Ministries and administrative organs by the MIC.

173. As a conclusion, EU laws and the ECHR, in the jurisprudence of their respective Courts, are establishing standards and guarantees according to which the oversight has to be complete, neutral and independent. The EDPB notes that the PPC does not have supervisory powers in matters related to law enforcement. Furthermore, if the oversight conducted by the Diet, the National and Prefectural Safety Commission appears to be neutral and independent, further clarification is needed about the supervisory powers of the Prefectural Public Safety Commissions.

4.1.3 Redress in the field of criminal law

174. The draft adequacy decision, complemented by Annex II, presents several avenues through which individuals can bring their complaints, both before independent authorities and before judges.

175. These avenues and the core elements of these procedures stemming from the available documentation are presented here after, following a brief overview of the available rights to clarify what data subjects can expect from public authorities in the context of data processing in the field of criminal procedures.

4.1.3.1 Available rights of data subjects in the context of criminal procedures

176. In order to obtain redress, data subjects need to have rights under the law to be able to claim they were not respected. Therefore, the EDPB also assessed the available rights in the context of criminal procedures presented in the draft adequacy decision.

[76] See Annex II p. 10.
[77] See Annex II p. 11.

4.1.3.1.1 General limitations to the rights of data subjects under the APPIHAO

177. In its draft adequacy decision, the COM refers to and relies on general data protection principles which public authorities have to respect, once they have collected personal data. These principles are also further outlined in the Annex II so that the EDPB has decided to also comment on them.

178. Concerning available rights, the EDPB notes that, according to Annex II of the draft Adequacy decision, some of the general rights provided to data subjects in the context of data processed by Administrative organs, remain available also in the context of criminal investigations. However, additional limitations with regard to the collection and further handling of personal information in this context also follow from the APPIHAO itself.

179. These limitations, which also appear to apply both in the context of data collected on the basis of a warrant as well as on the basis of an enquiry sheet in the context of voluntary disclosure, raise questions concerning several aspects.

180. Concerning the principle of purpose limitation, although in principle administrative organs are required to specify the purpose for which they retain personal data, and shall not retain them beyond the scope necessary for the achievement of the purpose of use specified, they can change the purpose if it is "what can reasonably be considered as appropriately relevant for the original purpose".

181. The APPIHAO also provides for the principle of non-disclosure, according to which an employee shall not disclose the acquired personal information to another person without a justifiable ground or use such information for an unjust purpose. However, no additional information is provided concerning the interpretation of what "justifiable ground" or "unjust purpose" could cover, so that further clarification would be necessary for the assessment.

182. Article 8(1) of the APPIHAO also lays down the prohibition to use or disclose data "except as otherwise provided by laws and regulations". Nevertheless, although this provision is not in principle contrary to the level of protection afforded under EU law, the EDPB lacks additional elements concerning the extent to which any supervision or checks is exercised when disclosure is provided by laws or regulations. In addition, under Article 8(2), additional exceptions apply to this rule where "such exceptional disclosure is not likely to cause unjust harm to the rights and interests of the data subject or a third party". Without any further elements on this point, this exception, which relies on the unclear notion of "unjust" harm, needs further clarification, if it is narrow enough.

183. Lastly, Article 9 of the APPIHAO provides for additional restrictions on the purpose or method of use or any other restrictions, to be imposed by the head of an administrative organ where retained personal information is provided to another person. As the notions of "any other necessary restrictions" and "provided to another person" are very broad, these additional restrictions to the rights of data subjects raise concerns without further clarifications on the scope of this provision.

184. While the EDPB is fully aware that access rights and other data protection principles are also limited in criminal proceedings under EU law, additional safeguards are provided when such limitations are foreseen, including in terms of supervision, oversight and redress. In the absence of sufficient case law on these limitations or additional elements to clarify the scope of these provisions, the EDPB is not in a position to assess whether these limitations to the rights of data subjects are limited to what would be considered strictly necessary and proportionate under EU law, and would thus be essentially equivalent to the rights provide to the EU data subjects.

4.1.3.1.2 Additional limitations to the rights of the APPIHAO deriving from the Code of Criminal Procedure and the Prefectural Police ordinances

185. The EDPB notes that although the APPIHAO seems to be applicable to all processing by administrative organs in Japan, some important limitations to the rights of data subjects derive from specific legislations. In particular, Article 53 (2) of the Code of Criminal Procedure[78] provides that "personal information recorded in documents relating to trials and seized articles" are excluded from the scope of application of the individual rights in Chapter IV of the APPIHAO. Concretely, the EDPB therefore understands that in the context of criminal procedures, data subjects do not benefit from the rights to information, access, rectification or erasure for personal data recorded in documents relating to trials and seized articles.

186. With regards to these limitations, the EDPB understands that they apply in the context of data collected on the basis of warrants, as well as in the context of data collected under the voluntary disclosure through enquiry sheets (see below). Indeed, the legal basis of the two procedures to access data (through a warrant and through an enquiry sheet) being provided in the code of criminal procedure, Article 53-2 of this code appears to apply to both types of collection. However, as Article 53-2 refers to the articles "seized" it could be clarified whether the limitations to the rights foreseen under this provision do apply also in the context of voluntary disclosure.

187. The EDPB regrets not to be provided with the ordinances of the Prefectural Police, which are said to be protecting personal information, rights and obligations equivalent to the APPIHAO. Given both the unclarities regarding the interpretation of the APPIHAO and the unavailability of the Prefectural Police ordinances, the EDPB wonders, if the granted rights to the individuals in this context, and the additional oversight and/or redress mechanisms are sufficient to compensate the absence of rights.

4.1.3.2 Redress through independent authorities redress

4.1.3.2.1 Administrative redress

188. The EDPB notes that the administrative organs collecting data, such as the Prefectural Police, are competent to deal with requests stemming from individuals concerning their – limited – rights with regards to their data collected as part of criminal investigations (see above concerning the rights available), which appear to include both the collection of data based on a warrant and on enquiry sheets. Concretely, these rights seem to be limited to general principles, such as the necessity of data retention, in connection with the purpose (see Article 3.1 APPIHAO), the purpose limitation principle (Article 4) or the accuracy of the data (Article 5), while individual rights such as the right to information, access, rectification or erasure are excluded for personal data recorded in documents relating to trials and seized articles[79]. Although these organs cannot be considered as independent and therefore as providing independent redress or oversight, the EDPB welcomes this avenue. However, it stresses that complaints filed in this context remain limited to very few rights of the data subjects given the limitations of rights provided by the APPIHAO.

189. Furthermore, as "personal information recorded in documents relating to trials and seized articles" are excluded from the scope of application of the individual rights in Chapter IV of the APPIHAO pursuant to Articles 53-2 of the Code of Criminal Procedure, the possibilities to request access to personal information are also limited to the procedures foreseen under other provisions of this Code of Criminal Procedure. It seems that only victims, suspected or accused persons can act in this context, and still,

[78] Available here http://www.japaneselawtranslation.go.jp/law/detail/?printID=&id=2283&re=02&vm=02 and quoted in Annex II of the draft adequacy decision, footnote 25.

[79] See supra concerning the limitations to APPIHAO and in particular see article 53-2 of the Code of Criminal Procedure (not provided but quoted in annex II of the draft adequacy decision, footnote 25).

depending on the stage of the criminal procedure. Therefore, the EDPB is concerned that no general right to access and/or rectify or delete information is available to data subjects under Japanese law in the context of criminal procedure, and that all redress avenues available imply to be either a victim (in which case the person would probably know that his/her data were collected) or a suspect or accused person, or the demonstration of a damage, while data subjects should also have the right to have access to their data and possibly to have their data rectified or deleted when they did not suffer any damage (yet possibly) and/or when they are neither a victim, a suspect or an accused person, but witnesses for instance.

4.1.3.2.2 Administrative redress through the Prefectural Public Safety Commissions

190. In addition, the Prefectural Public Safety Commissions appear to be competent to deal with complaints. Based on Article 79 of the Police law referred to in the draft adequacy decision, individuals can complaint against any illegal or improper behaviour of an agent in the execution of his/her duties.

191. The EDPB seeks clarification whether any "illegal" processing of personal data qualifies for an "illegal or improper behaviour of an agent" and on the demonstration of a disadvantage which seems required from the data subject. Indeed, the notice issued by the NPA to the Police and Prefectural Public Safety Commissions on the proper handling of complaints regarding the execution of duties by police officers limit the complaints to concrete claims concerning "correction for any specific disadvantage that has been inflicted as the result of an illegal or inappropriate behaviour, or failure to take a necessary action, by a police officer in his/her execution of duty" and the possibility to "file grievance/discontent about inappropriate mode of duty execution by a police officer". It is expressly clarified that "complaints on non-performance of a police officer concerning any matter that is not considered to fall under a police officer's duty, and also those expressing a general opinion or a proposal, not directly affecting the complaining party itself, shall be excluded".

192. Concerning the procedural requirements to file a complaint, although they have to be filed in writing, the EDPB notes that assistance for writing the complaint is provided in this context under Japanese law, including for foreigners. In addition, the Japanese government seems to have also entrusted the PPC with the duty to provide assistance to EU data subjects to handle and resolve complaints in this field, which the EDPB welcomes. The EDPB underlines that in its understanding, in this context, the PPC will only act as a point of contact between the EU data subjects and the competent authorities in Japan.

193. The results of the Prefectural Public Safety Commission following a complaint shall not be noticed in cases listed in Article 79-2 of the Police Act, which includes the case where the current "resident of the complainant is unknown". The EDPB acknowledges that the reference to the resident does not imply that in all cases EU data subjects would therefore be excluded from the notification of the results of their complaints on the ground they are not residing in Japan.

4.1.3.2.3 Ad Hoc mechanism implying the PPC

194. In view of the findings described above, The EDPB welcomes that the Japanese government and the EU Commission have agreed on an additional redress mechanism providing EU individuals with an additional avenue for redress in Japan through which individuals can also seek redress against unlawful or improper investigations by public authorities. The EDPB also notes and welcomes that the requests can be lodged with the PPC, rather than with another government official, thereby extending the scope of competence of the PPC to the area of law enforcement and national security.

195. The focus of the EDPB, when analysing the new mechanism, has been to understand the powers the PPC has in this context.

196. Even though the language is not entirely clear, the EDPB understands that the additional redress mechanism does not require "standing" in the meaning that the requestor is not required to show that her personal data is likely to have been subjected to surveillance by a Japanese authority. The EDPB would still like to request confirmation by the Commission.

197. In line with its assessment of the Ombudsperson mechanism, created under the Privacy Shield, the EDPB stresses the need for effective powers of the addressee of the request, in this case the PPC, in order to consider the redress mechanism as essentially equivalent to an effective remedy in the meaning of Art. 47 of the Charta on Fundamental Rights.

198. When explaining the redress mechanism, the Japanese government refers to Art. 6, 61 (ii) and 80 APPI and lays out these powers in Annex II. It is the understanding of the EDPB that the procedure as described in Annex II specifies or extends the powers of the PPC, as the language in Art. 6, 61 (ii) and 80 APPI is rather vague and general. To the extent Annex II specifies or extends the powers of the PPC, the EDPB would like to ask for clarification that the other agencies of the Japanese government are bound by them.

199. On the basis of the procedure in Annex II, the EDPB notes that the competent public authorities in Japan are required to cooperate with the PPC, "including by providing them with the necessary information and relevant material, so that the PPC can evaluate whether the collection or the subsequent use of personal information has taken place in compliance with the applicable rules". For the assessment of the effectiveness of the system, it is thus important to refer again to the powers that those competent authorities have with which the PPC cooperates. It is the understanding of the EDPB that those powers would not be extended through the reassurances in Annex II.

200. The EDPB also notes that, if a violation of the rules has been identified, "the cooperation by the concerned public authorities with the PPC includes the obligation to remedy the violation", which expressly includes the deletion of the data collected in violation of the applicable rules. The EDPB understands that the obligations of the competent authority stem from the "cooperation with the PPC", rather than from a decision by the PPC.

201. Finally, the PPC will inform the requestor of the "outcome of the evaluation, including any corrective action taken where applicable." In addition, the PPC will inform the requestor about the "possibility of seeking a confirmation of the outcome from the competent public authority and about the authority to which such a request for confirmation shall be made."

202. In addition, the PPC has committed to assist the requestor with bringing further action under Japanese law, if the requestor is dissatisfied with the outcome of the procedure.

203. In light of the need to have an effective redress mechanism essentially equivalent to the EU standards, the EDPB nevertheless wonders if the PPC has any specific powers other than evaluating whether the collection or the subsequent use of personal information has taken place in compliance with the applicable rules and calling on the competent authorities to use their respective powers and to deal with complaints forwarded to them by the PPC. Should the PPC only act as a contact point for the EU individuals, the EDPB would consider this as insufficient to provide for an effective redress mechanism essentially equivalent to the EU standards. The EDPB thus calls on the Commission to provide clarifications on the points mentioned in this sub-chapter, in particular on whether and how the mechanism extends the obligations of competent authorities, how they are bound by it, and how the PPC can effectively ensure compliance and not only acting as a contact point for EU individuals.

4.1.3.3 Judicial redress

4.1.3.3.1 Quasi complaint mechanism

204. The so-called "quasi-complaint" procedure allows to act against compulsory collection of information based on a warrant to have an illegal seizure rescinded or altered.

205. This avenue implies the individual is aware of the data being seized. However, the EDPB understands that the procedure for the collection of data based on a warrant is not notified to the data subject. Equally, it understands that voluntary disclosure does not imply that companies requested have the obligation to inform the data subjects of requests received and complied with. Therefore, although it is stressed in the Annex II that "such a challenge can be brought without the individual having to wait for the conclusion of the case", in practice, apart for warrants authorising wiretapping, for which it is indicated that the Law provides for a notification requirement[80], this avenue seems to be effectively available only once the data subject got aware of the collection through a case brought against her or him.

4.1.3.3.2 Injunctive relief

206. In addition, in order to obtain the deletion of data collected through a criminal procedure (the so-called "injunctive relief"), or to obtain compensation of damages, individuals can also bring civil actions before a judge.

207. As regards compensation, the EDPB notes that the procedure seems to be circumscribed to situations where a public officer in the course of his duties, unlawfully and with fault (intentionally or negligently) inflicted damage on the individual concerned. In the understanding of the EDPB, the damage appears to include moral damages. It is however not set out in further detail what needs to be demonstrated by the individual that he/she suffered a damage. The EDPB was not in a position to assess the case law concerning the award of compensation, and is therefore unable to assess whether this avenue provides for an effective remedy in case of damage.

208. With regards to the "injunctive relief", the EDPB also notes that to file a request, the individual should first be aware that his/her data were collected and that they are still retained. Therefore, given the limited rights of information and access of individuals in the context of criminal investigations and procedures, the efficiency of the procedure appears to be rather limited too.

4.1.3.4 Overall assessment of the avenues for redress

209. Following the assessment of all the redress avenues open for individuals under Japanese law as well as to the EU data subjects before the PPC, the EDPB welcomes the *ad hoc* dispute resolution mechanism, involving the PPC. It has an added value for EU data subjects, in particular since it allows them to understand which avenues are available for them to obtain redress and/or compensation, as well as to present their requests according to the applicable procedural requirements under Japanese law. However, further clarifications are necessary, in particular on whether and how the mechanism extends the obligations of competent authorities, how they are bound by it, and how the PPC can effectively ensure compliance, in order to ensure that this new mechanism provides for effective redress.

210. This assessment shows that no redress mechanism in Japanese law appears to allow for access, rectification or deletion of data for data subjects who are not victims, suspects or accused in the context of a criminal procedure, for instance to remedy unlawful collection or retention of their data.

[80] Article 23 of the Wiretapping Act is mentioned page 33 of the draft adequacy decision, however the EDPB was not provided with this text and is therefore unable to assess to which extent this notification obligation applies and in which cases it might be limited.

It also shows that all redress and compensation mechanisms and procedures available under Japanese law for victims, suspects or accused person imply the knowledge of the collection of data, which appears to be limited in practice since limited rights of access and information are provided for them. In addition, further clarification appears necessary about the demonstration of an illegal behaviour on the part of the authorities, in particular whether such behaviour includes any illegal processing of personal data, or of a damage suffered by the individual.

211. Therefore, without further documentation and elements, the EDPB is concerned as to whether redress under Japanese law and under the draft adequacy decision is sufficiently effective compared to the standards in EU law.

4.2 Access for national security purposes

4.2.1 Scope of surveillance

212. In the draft adequacy decision, the chapter on "access and use by Japanese public authorities for national security purposes" is introduced by a general statement, in line with the reassurance provided by the Japanese government in Annex II, according to which no Japanese law would provide and thus permit "compulsory requests for information or "administrative wiretapping" outside criminal investigations". As a conclusion, it is said that "on national security grounds information may only be obtained from an information source that can be freely accessed by anyone or by voluntary disclosure. This excludes any covert surveillance activities in this area. Business operators receiving a request for voluntary cooperation (in the form of disclosure of electronic information) are under no legal obligation to provide such information."[81]

213. Within these limitations, four government entities are listed which have the power to collect electronic information held by Japanese business operators on national security grounds. With regard to the Ministry of Defence, as one of those four entities, it is said that it "only has authority to collect (electronic) information through voluntary disclosures".[82]

214. For its assessment of the general setup of data collection for the purpose of national security, the EDPB wishes to recall the first of the four so called "essential guarantees", according to which "processing should be based on clear, precise and accessible rules".[83] More specifically, the ECHR has been very clear that surveillance programs are only "in accordance with the law" if the surveillance measures "have some basis in domestic law". The court has clarified that compatibility with the rule of law requires the law authorizing the measure must be accessible and foreseeable as to its effects. Referring to the risk of arbitrariness, the court has required "clear, detailed rules on secret surveillance measures"; "sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measure".[84]

215. For the application of these essential guarantees to the legal system of Japan, the EDPB is aware not only of the fact that, in matters of national security, states have a broad margin of appreciation, recognized by the European Court of Human Rights. Also, national security powers reflect the historical experiences nations make. The EDPB thus understands that, as emphasized by the Japanese government, after World War II, Japanese national intelligence agencies have been equipped with more limited powers than in other states.

[81] Adequacy decision, paragraph 151.
[82] Adequacy decision, paragraph 153.
[83] WP29, WP 237: Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees).
[84] See e.g. Big Brother Watch and others v. the United Kingdom, paragraph 305.

216. In the reading of the EDPB, the draft adequacy decision, in line with the reassurance by the Japanese government, suggests that Japanese government entities do not run programs, which strategically monitor or broadly surveille (internet) communication. As said above, the Japanese government has given reassurance, in a letter signed by the Minister of Justice, that "on national security grounds information may only be obtained from an information source that can be freely accessed by anyone or by voluntary disclosure".

217. As to the legal basis of the Ministry of Defence, the EDPB notes that the draft adequacy decision includes general information about its powers and quotes its mission "to conduct such affairs as related thereto in order to secure national peace and independence, and the safety of the nation". However, the EDPB has not been provided with an English translation of the legal basis.

218. At the same time, the EDPB is aware of reports published in different media suggesting that surveillance programs are run by the Directorate for Signals Intelligence of Japan's Ministry of Defense (MOD).[85] In the report, it is also claimed that the Japanese Ministry of Defense, while refusing to discuss specifics of the report, has "acknowledged that Japan has "offices throughout the country" that are intercepting communications" and that those "would be focused on military activities and "cyberthreats" and are "not collecting the general public's information". The latter statement (that the MOD does not collect information on the general public) is made part of the restatement by the Japanese government.

219. It stands that the Japanese government has restated, in a letter signed by the Minister of Justice, that the MOD does not collect information on the general public.

220. It is beyond the task of the EDPB to make a general assessment of the possible surveillance capabilities of the Japanese government. Those activities are only important for its assessment if they are relevant for the transfer of personal data between the EU and Japan. In this context, the EDPB would like to reaffirm its approach already adopted by its predecessor when asked to opine on the EU-U.S. Privacy Shield. When giving an opinion on the Privacy Shield, the WP29 included in its analysis the powers and limits of the U.S. to conduct surveillance of data "on its way" to the U.S.[86] Applying the same standard for the adequacy decision on Japan, the EDPB takes the view that information on the powers of Japanese authorities to surveille data "on its way" to Japan are relevant. Should these surveillance powers exist, also the decision in Big Brother Watch by the ECHR appears to suggest that such powers would have to be regulated in accordance with the standards established by the ECHR.

221. As a consequence, if interceptions were limited to the "assistance of military action", they may well not be relevant for the assessment of the adequacy decision. It is thus the interest of the EDPB to receive clarifications on the surveillance measures by Japanese governmental entities. In this respect, such clarification would be welcome in order to determine whether data undergoing transfer under

[85] In May 2018, the online news publication "The Intercept" published a report titled "The untold story of Japan's secret spy agency".
[86] See WP255, EU-U.S. Privacy Shield –First annual joint review, adopted on 28 November 2017, p. 16: "WP29 is of the view that the analysis of the laws of the third-country for which adequacy is considered, should not be limited to the law and practice allowing for surveillance within that country's physical borders, but should also include an analysis of the legal grounds in that third-country's law which enable it to conduct surveillance outside its territory as far as EU data are concerned. As already underlined in its previous opinion, "It should be clear that the Privacy Shield Principles will apply from the moment the data transfer takes place, which means including as regards data "on its way" to that country."

this adequacy framework could be the subject of access for national security purposes by the Japanese competent authorities in that field.

4.2.2 Voluntary disclosure in case of national security

222. The draft adequacy decision states that the four government entities only have the authority to collect (electronic) information by voluntary disclosure. According to the draft decision and Annex II, there are some limitations on statutory grounds, which means that the collection of data is limited to what is necessary for the execution of the tasks by the entities.

223. In the area of criminal law, as mentioned in the section about law enforcement, voluntary disclosure is only permissible as part of a criminal investigation, and thus presupposes a concrete suspicion of a crime that is already committed. Investigations in the area of national security differ from investigations in the area of law enforcement. The EDPB acknowledges that, according to Annex II, the central principles of "necessity for investigation" and "appropriateness of method" similarly apply in the area of national security and have to be complied with taking appropriate account of the specific circumstances of each case.[87] It regrets that the application is not further clarified, including by way of further reference to case law. Nevertheless the EDPB states, that the use of this procedure has to be proportionate or necessary.

224. According to the draft decision, when personal information has been collected ('obtained'), its handling is governed by the APPIHAO except for the Prefectural Police.[88] Annex II states that the handling of personal information by the Prefectural Police is governed by prefectural ordinances that stipulate principles for the protection of personal information, rights and obligations equivalent to the APPIHAO.[89] Because there are no English translations available for these ordinances, the EDPB is not in a position to assess whether the principles are equivalent to those of the APPIHAO.

225. For the other remarks on voluntary disclosure, reference is made to the section on law enforcement.

4.2.3 Oversight

4.2.3.1 General Points

226. The four government entities empowered to collect electronic information held by Japanese business operators on national security grounds, are: (i) the Cabinet Intelligence & Research Office (CIRO); (ii) the Ministry of Defence ("MOD"); (iii) the police (both National Police Agency (NPA)[90] and Prefectural Police); and (iv) the Public Security Intelligence Agency ("PSIA").

227. According to the draft adequacy decision, these government entities are subject to several layers of oversight from three branches of the government[91]. The EDPB notes that there are oversight mechanism within the legislative branch (Japanese Diet) and the executive branch (Inspector General's Office of Legal Compliance (IGO), the Prefectural Public Safety Commissions and the Public Security Examination Commission). The EDPB stresses that the COM should clarify the judicial oversight *(ex-officio/*guarantee C of the WP 237; for redress, there is a separate chapter in the draft decision and an extra guarantee in the WP 237) of the above-mentioned government bodies, as it is unclear whether

[87] See Annex II, pp. 23.
[88] Adequacy decision, paragraph 118 and 157.
[89] See Annex II, pp. 3.
[90] However, according to the information received, the main role of the NPA is to coordinate investigations by the various Prefectural Police departments and its information collection activities are limited to exchanges with foreign authorities.
[91] See Annex II, pp. 39.

there is such a judicial oversight in the area of collection of personal information for national security purposes without compulsory means.

4.2.3.2 Oversight by the Japanese Diet

228. The EDPB notes that the Japanese Diet may conduct investigations in relation to the activities of public authorities, therefore also for all of the aforementioned government entities. Furthermore, the diet may also request the production of documents and the testimony of witnesses (*Article 62 of the Japanese Constitution, Article 104 Diet Law*). The EDPB also remarks that according to *Articles 74 and 75 Diet Law*, Diet members may ask written questions to the Cabinet which may end in an answer from the Cabinet (*Article 75 Diet Law*). Finally, it is as well noted that there are specific reporting obligations for e.g. the Public Security Intelligence Agency (PSIA) (Article 36 SAPA/Art 31 ACO), by means of a yearly report to the Diet. Such a report was not provided to the EDPB.

4.2.3.3 Oversight by the Inspector General's Office of Legal Compliance (IGO)

229. The EDPB notes that there is an oversight body for the MOD, called IGO. The EDPB was not provided with the MOD Establishment Act (Act for the Establishment of the MOD), but only with the representations in Annex II to the draft decision. Pursuant to Annex II, the IGO is an independent office within the MOD, which is under the direct supervision of the Minister of Defense according to Article 29 of the MOD Establishment Act. The IGO has the powers of carrying out inspections of compliance with laws and regulations by officials of the MOD (« so called « Defense Inspections »), across the entire ministry including the Self-Defense Forces.

230. Pursuant to the Annex II, the IGO performs its duties independently from MOD's operational departments. The EDPB notes that the IGO is an *internal* oversight body.

231. Inspections lead to findings and, with the intention to ensure compliance, measures which are directly reported to the Minister of Defence. Based on the report of the IGO, the Minister of Defence may issue orders to implement the measures necessary to remedy the situation. The Deputy Vice minister of Defence is responsible for implementing these measures and must report to the Minister of Defence on the status of such an implementation.

232. Analysing Annex II, without being provided with the legal provisions (MOD Establishment Act) for this considerations, the EDPB welcomes the possibility of ordering necessary compliance measures to remedy the situation. However, the EDPB raises doubts regarding the independence of the IGO, as it is an office within the MOD and is under direct supervision of the Minister of Defence pursuant to Annex II (according to the *WP 237* « *functional independence is not by itself sufficient to protect that supervisory authority from all external influence* »).

233. In alignment to the case law of the ECHR and the *WP 237* respectively following the considerations of Annex II, the Inspector General can request for reports from the concerned office (documents, sites, explanations). Clarification as to whether the offices concerned are obliged to follow these requests or not and whether the requested documents include closed materials, like the *WP 237* mentions or not, appear necessary to the EDPB.

234. Although the EDPB welcomes that very senior legal experts (former Superintending Prosecutor) head the IGO, clarification about the manner of appointment of this supervisory body appears necessary.

4.2.3.4 Oversight by Public Security Examination Commission

235. According to Annex II (page 25), PSIA carries out regular and special inspections on the operations of its individual bureaus and offices (Public Security Intelligence Bureau, Public Security Intelligence Offices and Sub Offices, etc). For the purposes of the regular inspection, an Assistant Director General

and/or a Director are designated as inspectors. Such inspections should also concern the management of personal information.

236. Pursuant to recital 163 of the draft decision the *Public Security Examination* Commission operates as an independent ex ante oversight body for the PSIA, with regards to issues of the ACO[92] and SAPA[93]. The EDPB welcomes that.

237. Although the website of the Japanese Ministry of Justice provides some information[94], the EDPB is not in the position to carefully further assess the independency of the Public Security Examination Commission since it was not provided with the Act of the establishment of the Public Security Examination Commission[95] and the Rules of the Public Security Examination Commission[96].

4.2.3.5 Oversight by National Public Safety Commission, Prefectural Public Safety Commissions and the APPIHAO (executive)

238. See 3.1.2.2.1 (National Public Safety Commission), 3.1.2.2.2. (Prefectural Public Safety Commissions) and 3.1.2.2.4. (Executive).

4.2.3.6 Oversight by PPC

239. The EDPB invites the COM to either mention in Recital 164 that the PPC is not an oversight body for the aforementioned government entities and that it is only competent for the redress of the individuals or to move the passage in recital 164 about the PPC to the section « individual redress ».

4.2.4 Redress mechanism

240. For the analysis of the newly negotiated redress mechanism, reference is made to the section on law enforcement.

241. In addition, it is noteworthy that the Japanese law provides for a specific individual redress avenue available in the area of national security. It is the understanding of the EDPB that all individuals, including EU individuals, may generally request disclosure, correction (including deletion) or suspension of use from the administrative organs, also if those are processed for national security purposes. In case such a request is "rejected on the grounds that the concerned information is considered non-disclosable", an appeal for review may be lodged, and the "Information Disclosure and Personal Information Protection Review Board" has to be consulted. The Board is composed of members appointed by the Prime Minister with the consent of both Houses, equipped with investigative powers, and concludes with a written report for the concerned individual, which is not

[92] Act on the Control of Organizations Which Have Committed Acts of Indiscriminate Mass Murder (Act No. 147 of December 7, 1999).
[93] Subversive Activities Prevention Act(Act No. 240 of July 21, 1952).
[94] See http://www.moj.go.jp/ENGLISH/MEOM/meom-01.html (September 2018): the extra-ministerial organ "*is composed of a chairperson and six members. They are selected from among persons of good character who are capable of making a fair judgment on the control of organizations and those who have ample knowledge and experience of both law and society. They are appointed by the Prime Minister and must be approved by both houses of the Diet. With regard to the application of the previously mentioned laws (SAPA/ACO), the members perform their duties quite independently, free from any direction or supervision of the Prime Minister or the Minister of Justice.*"
[95] http://www.japaneselawtranslation.go.jp/law/detail_main?re=&vm=2&id=613 (September 2018).
[96] Article 28 ACO.

legally binding, but almost always followed.[97] According to Annex II, there were only two out of 2000 cases, where an administrative authority took a decision that differed from the Board's conclusion.[98]

242. It appears to follow from the explanation provided that the review is not available, if the information can be "disclosed" but the individual is dissatisfied with the outcome. The EDPB acknowledges this avenue for redress, but would like to seek further clarification on the latter aspect, which would significantly limit its scope.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

[97] Annex II, p. 25, 26. Act for Establishment of the Information Disclosure and Personal Information Protection Review Board, Art. 4, 9, 11.
[98] Annex II, footnote 35.



Opinia 23/2018 w sprawie wniosków Komisji dotyczących europejskiego nakazu wydania dowodów i europejskiego nakazu zabezpieczenia dowodów w sprawach karnych (art. 70 ust. 1 lit. b)

Przyjęta dnia 26 września 2018 r.

Spis treści

Wprowadzenie ... 3
1. Podstawa prawna wniosku dotyczącego rozporządzenia (art. 82 TFUE) ... 4
2. Niezbędność wprowadzenia dowodów elektronicznych a traktaty o pomocy prawnej i europejski nakaz dochodzeniowy ... 5
a) Niezbędność wprowadzenia dowodów elektronicznych a zabezpieczenia przewidziane w europejskim nakazie dochodzeniowym i traktatach o pomocy prawnej ... 5
b) Rezygnacja z zasady podwójnej karalności ... 7
c) Konsekwencje zwracania się bezpośrednio do przedsiębiorstw ... 8
3. Nowa podstawa jurysdykcji oraz tzw. pominięcie kryteriów terytorialnych ... 8
4. Pojęcie „dostawca usług" należy ograniczyć lub uzupełnić dodatkowymi zabezpieczeniami praw osób, których te dane dotyczą ... 10
5. Pojęcia „siedziba" i „przedstawiciel prawny" w kontekście przedmiotowych wniosków powinny być wyraźnie rozróżnione od tych pojęć w ujęciu RODO ... 11
a) Zakład ... 11
b) Przedstawiciel prawny ... 12
6. Nowe kategorie danych ... 12
7. Analiza procedur europejskiego nakazu wydania dowodów i europejskiego nakazu zabezpieczenia dowodów ... 14
a) Należy podnieść progi powodujące wydanie nakazu, a na wydanie nakazu powinny wydawać zezwolenia sądy ... 15
b) Terminy udostępniania danych powinny być uzasadnione ... 16
c) Europejski nakaz wydania dowodów i europejski nakaz zabezpieczenia dowodów można stosować do żądania danych osoby, której te dane dotyczą, z innego państwa członkowskiego jedynie po poinformowaniu właściwych organów tego państwa członkowskiego, w szczególności w odniesieniu do danych dotyczących treści ... 17
d) Europejskie nakazy zabezpieczenia nie mogą być wykorzystywane do obchodzenia obowiązków dostawców usług w zakresie zatrzymywania danych ... 18
e) Poufność i informowanie użytkowników ... 18
f) Procedura przymusowego wykonania nakazu w przypadku, gdy dostawca usług odmówił jego wykonania ... 18
g) Przymusowe wykonywanie a konflikt obowiązków wynikający z przepisów prawa państwa trzeciego (art. 15–16) ... 19
h) Bezpieczne przekazywanie danych w ramach wykonania nakazu ... 21
Podsumowanie ... 22

Europejska Rada Ochrony Danych

Uwzględniając art. 70 ust. 1 lit. b) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE,

PRZYJMUJE NASTĘPUJĄCĄ OPINIĘ:

Wprowadzenie

W kwietniu 2018 r. Komisja przedstawiła wniosek dotyczący rozporządzenia w sprawie europejskiego nakazu wydania dowodów i europejskiego nakazu zabezpieczenia dowodów w sprawach karnych oraz wniosek dotyczący dyrektywy ustanawiającej zharmonizowane przepisy dotyczące mianowania przedstawicieli prawnych w celu gromadzenia dowodów na potrzeby postępowań karnych. Te dwa wnioski COM (2018) 225 final i COM (2018) 226 final uzupełniają się. Ogólnym celem Komisji jest poprawa współpracy między organami państw członkowskich a dostawcami usług, w tym dostawcami usług spoza UE, a także zaproponowanie rozwiązań problemu określania i egzekwowania jurysdykcji w cyberprzestrzeni.

W projekcie rozporządzenia ustanowiono zasady i procedury mające zastosowanie do wydawania, doręczania i egzekwowania wobec podmiotów świadczących usługi łączności elektronicznej nakazów wydania dowodów i nakazów zabezpieczenia dowodów. W projekcie dyrektywy natomiast przewidziano minimalne zasady dotyczące mianowania przedstawiciela prawnego dla dostawców usług niemających siedziby w UE.

W listopadzie 2017 r.[1], zanim Komisja przedłożyła projekt wniosku, Grupa Robocza Art. 29 przypomniała o konieczności zapewnienia, aby wszelkie wnioski legislacyjne były w pełni zgodne z obowiązującym dorobkiem prawnym UE w dziedzinie ochrony danych, jak również ogólnie z unijnym prawem i orzecznictwem.

W szczególności Grupa Robocza Art. 29 ostrzegła przed ograniczeniami praw do ochrony danych i prywatności w odniesieniu do danych przetwarzanych przez dostawców usług telekomunikacyjnych i usług społeczeństwa informacyjnego, zwłaszcza gdy dane te są dalej przetwarzane przez organy ścigania, przypomniała o konieczności zapewnienia spójności wszelkich instrumentów UE z obowiązującą konwencją budapeszteńską Rady Europy o cyberprzestępczości oraz z dyrektywą UE w sprawie europejskiego nakazu dochodzeniowego (END), a także zaleciła doprecyzowanie odpowiednich przepisów proceduralnych regulujących dostęp do dowodów elektronicznych na szczeblu krajowym i unijnym w celu zapewnienia, aby nowy instrument nie przyznawał organom nowych uprawnień, których nie miałyby one wewnętrznie. Oprócz tych ogólnych uwag Grupa Robocza Art. 29 przedstawiła uwagi na temat wariantów ustawodawczych rozpatrywanych wówczas przez Komisję w odniesieniu do kategorii tych danych oraz odpowiadających im zabezpieczeń dostępu do nich, na temat możliwości kierowania nakazów wydania dowodów/wniosków o wydanie dowodów w celu nakłonienia dostawców usług spoza UE do udostępnienia danych, a także na temat materialnych i proceduralnych warunków niezbędnych zabezpieczeń związanych z bezpośrednim dostępem do danych.

Teraz, gdy przedstawiono już gotowe wnioski dotyczące dostępu do dowodów elektronicznych, EROD pragnie w sposób bardziej szczegółowy przeanalizować zaproponowane instrumenty prawne pod kątem ochrony danych.

[1] Zob. oświadczenie Grupy Roboczej Art. 29 (http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48801)

1. Podstawa prawna wniosku dotyczącego rozporządzenia (art. 82 TFUE)

Podstawę prawną zaproponowaną w projekcie rozporządzenia w sprawie dowodów elektronicznych stanowi art. 82 ust. 1 TFUE dotyczący współpracy sądowej w sprawach karnych, który stanowi, że:

> *1. Współpraca wymiarów sprawiedliwości w sprawach karnych w Unii opiera się na zasadzie wzajemnego uznawania wyroków i orzeczeń sądowych oraz obejmuje zbliżanie przepisów ustawowych i wykonawczych Państw Członkowskich w dziedzinach, o których mowa w ustępie 2 i w artykule 83.*
>
> *Parlament Europejski i Rada, stanowiąc zgodnie ze zwykłą procedurą ustawodawczą, przyjmują środki mające na celu:*
>
> *a) ustanowienie zasad i procedur zapewniających uznawanie w całej Unii wszystkich form wyroków i orzeczeń sądowych;*
>
> *b) zapobieganie sporom o jurysdykcję między Państwami Członkowskimi i ich rozstrzyganie;*
>
> *c) wspieranie szkolenia sędziów i innych pracowników wymiaru sprawiedliwości;*
>
> *d) ułatwianie współpracy między organami sądowymi lub równoważnymi organami Państw Członkowskich w ramach ścigania karnego i wykonywania orzeczeń.*

Jak podkreśliła Komisja w ocenie skutków towarzyszącej wnioskom, „art. 82 ust. 1 stanowi, że współpraca wymiarów sprawiedliwości w sprawach karnych opiera się na zasadzie wzajemnego uznawania. Wskazana podstawa prawna obejmowałaby ewentualne uregulowanie w sprawie bezpośredniej współpracy z usługodawcami, w ramach której organ wydającego państwa członkowskiego występowałyby bezpośrednio do danego podmiotu (dostawcy usług) w państwie wykonującym, a nawet nakładałby na niego obowiązki. Tym samym mechanizm wzajemnego uznawania nabrałby nowego wymiaru wykraczającego poza tradycyjną unijną współpracę sądową, która opierała się dotychczas na procedurach angażujących dwa organy sądowe – jeden w państwie wydającym i drugi w państwie wykonującym."(podkreślenie dodane)

Biorąc pod uwagę nowatorskie zastosowanie wskazanej podstawy prawnej, które polega na możliwości bezpośredniego występowania organów publicznych do podmiotów prywatnych, Europejska Rada Ochrony Danych wyraża ubolewanie, że Komisja nie przedstawiła ani pogłębionej analizy, ani oceny tego podejścia.

Co więcej, jak już podkreśliła to grupa robocza w swoim poprzednim oświadczeniu, tak i obecnie zdaniem EROD zachodzą wątpliwości co do prawidłowego zastosowania tej podstawy prawnej. Wątpliwości te wzmacnia wywód Trybunału Sprawiedliwości Unii Europejskiej i jego rzecznika generalnego zawarty w opinii 1/15. Wśród uwag Trybunału odnoszących się do kwestii prawidłowości zastosowania art. 82 jako podstawy prawnej dla przewidywanej umowy między Kanadą a Unią Europejską o przekazywaniu i przetwarzaniu danych PNR, Trybunał podkreślił, że kanadyjski właściwy

organ *„nie jest [..] ani organem sądowym, ani organem mu równoważnym"*[2]. W kontekście przedstawionych wniosków dotyczących dowodów elektronicznych jednym z głównych celów proponowanych regulacji wydaje się być, jak stwierdziła Komisja, uniknięcie „zbyt uciążliwej" współpracy sądowej. W związku z tym wniosek oparto na zasadzie, zgodnie z którą współpraca powinna odbywać się pomiędzy organem a usługodawcą, a nie pomiędzy dwoma organami. Zgodnie z przewidywaną procedurą to przede wszystkim podmioty prywatne mają być odbiorcami wniosków pochodzących od organów sądowych oraz do nich należałoby udzielanie odpowiedzi na te wnioski.

EROD zauważa, że wykonanie nakazu wydania dowodów lub nakazu zabezpieczenia dowodów mogłoby pociągać za sobą konieczność zaangażowania organu otrzymującego w sytuacji, gdy usługodawca, który otrzymał wniosek, nie wykonuje nałożonego na niego obowiązku, co wywołuje konieczność zwrócenia się o wykonanie nakazu ex post. Jako że głównym celem ustanowionej procedury jest jednak, by nie angażować organu otrzymującego, zdaniem EROD wątpliwości budzi kwestia, czy omawiana procedura pomocnicza mogłaby uzasadniać stosowanie art. 82 jako jedynej podstawy prawnej dla tego instrumentu.

Dlatego też EROD uważa, że współpraca taka wymagałaby stosowania innej podstawy prawnej, natomiast art. 82 należy stosować wówczas, gdy na głównych etapach procedury odbywa się współpraca pomiędzy dwoma organami sądowymi.

2. Niezbędność wprowadzenia dowodów elektronicznych a traktaty o pomocy prawnej i europejski nakaz dochodzeniowy

EROD zauważa, że Komisja zobowiązuje się przeprowadzić przegląd przeszkód w prowadzeniu dochodzeń w sprawach karnych, w szczególności co do kwestii dostępu do dowodów elektronicznych. W uzasadnieniu Komisja przedstawiła kontekst wniosku oraz podkreśliła ulotność dowodów elektronicznych, ich znaczenie międzynarodowe, jak również konieczność dostosowania mechanizmu współpracy do warunków ery cyfrowej. Wnioski dotyczące rozporządzenia i dyrektywy w sprawie przekazywania i dostępu do dowodów elektronicznych nie zmierzają do zastąpienia wcześniejszych instrumentów współpracy w sprawach karnych, takich jak konwencja budapeszteńska, traktat o pomocy prawnej oraz europejski nakaz dochodzeniowy (dyrektywa END). Według Komisji wnioski dotyczące dowodów elektronicznych mają na celu usprawnienie współpracy sądowej w sprawach karnych pomiędzy organami i usługodawcami w Unii Europejskiej, jak również z państwami trzecimi, w szczególności ze Stanami Zjednoczonymi.

Ponieważ te nowe narzędzia będą specjalnie służyć przekazywaniu dowodów elektronicznych i uzyskiwaniu do nich dostępu, EROD oceni wartość dodaną instrumentów w porównaniu z dyrektywą END oraz traktatem o pomocy prawnej.

a) Niezbędność wprowadzenia dowodów elektronicznych a zabezpieczenia przewidziane w europejskim nakazie dochodzeniowym i traktatach o pomocy prawnej

[2] Zob. pkt 103 opinii 1/15 i pkt 108 opinii rzecznika generalnego w tej sprawie.

Główny argument Komisji na poparcie wniosków dotyczących dowodów elektronicznych to przyspieszenie procesu zabezpieczania i uzyskiwania dowodów elektronicznych przechowywanych przez lub będących w posiadaniu dostawców usług prowadzących działalność w innej jurysdykcji.

EROD ubolewa jednak, że w ocenie skutków nie wskazano na konieczność stworzenia nowego instrumentu służącego udostępnianiu dowodów elektronicznych. Co więcej, we wnioskach tych nie wykazano, że można było wykorzystać inne mniej ingerujące w prywatność środki, aby osiągnąć cel wniosku. Jednocześnie można było rozważyć rozwiązania alternatywne. Przykładowo można było rozważyć możliwość wprowadzenia zmian i ulepszeń w dyrektywie END, co tym samym pozwoliłoby spełnić szczególny wymóg wynikający z przepisów tej dyrektywy, a wiążący się z oceną potrzeb wprowadzenia w niej zmian do dnia 21 maja 2019 r[3]. Innym rozwiązaniem mogłoby być takie uregulowanie nakazów zabezpieczenia, aby można je było wykorzystywać w celu zamrożenia danych tak długo, na jak długo dany wniosek na podstawie traktatu o pomocy prawnej formalnie wydano. Warianty te umożliwiłyby utrzymanie zabezpieczeń przewidzianych w tych instrumentach przy jednoczesnym zagwarantowaniu, że poszukiwane dane osobowe nie zostaną usunięte.

EROD zauważa, że terminy ustanowione w dyrektywie END są dłuższe niż te określone we wniosku dotyczącym dowodów elektronicznych. I tak, organ wykonujący ma 30 dni na podjęcie decyzji w sprawie uznania wniosku[4], a następnie powinien wykonać nakaz w terminie 90 dni[5]. Zdaniem EROD przyznanie organom wykonującym END 30-dniowego terminu do namysłu stanowi kluczowe zabezpieczenie pozwalające tym organom ocenić, czy dany wniosek o wykonanie jest właściwie uzasadniony oraz czy spełnione zostały wszystkie warunki wydania i przekazania END[6].

EROD wyraża obawę, że 10-dniowy termin do wykonania zaświadczenia europejskiego nakazu wydania dowodów (EPOC), który zaproponowano we wnioskach dotyczących dowodów elektronicznych, nie daje organowi czasu do namysłu, uniemożliwiając dokonanie właściwej oceny tego, czy EPOC spełnia wszystkie kryteria oraz czy jest poprawnie wypełniony.

Dlatego też EROD zaleca, aby ustanowić termin dłuższy, który umożliwi odbiorcy EPOC rozważenie, czy wykonanie nakazu jest zasadne.

EROD zauważa, że w przypadku zaświadczenia europejskiego nakazu zabezpieczenia dowodów nie ma gwarancji, że zabezpieczenie danych będzie ograniczone do tego, co jest niezbędne do ich wydania. Okres zabezpieczenia danych może być bowiem dłuższy niż 60 dni, ponieważ organ wydający nie jest związany terminem co do powiadomienia adresata o odstąpieniu od wydania nakazu wydania dowodów lub jego wycofaniu. W związku z powyższym EROD zaleca, aby ustanowić co najmniej termin do odstąpienia przez organ wydający od wydania nakazu wydania dowodów lub jego wycofania w celu zachowania zgodności z ustanowioną w RODO zasadą minimalizacji danych[7].

Wreszcie EROD zauważa, że w dyrektywie END ustanowiono zwrot dowodów przez państwo wydające organowi wykonującemu[8]. Wniosek dotyczący rozporządzenia w sprawie dowodów elektronicznych jednak na temat takiej możliwości milczy. Co stanie się z dowodami elektronicznymi po ich przekazaniu organowi wydającemu, tego nie wiadomo.

[3] Zob. art. 37 dyrektywy.
[4] Art. 12 ust. 3 dyrektywy END
[5] Art. 12 ust. 4 dyrektywy END
[6] Art. 6 dyrektywy END
[7] Art. 5 ust. 1 lit. c) RODO.
[8] Art. 13 ust. 3 i 4 dyrektywy END.

Dlatego też EROD zaleca, aby wniosek dotyczący rozporządzenia zawierał więcej informacji na temat wykorzystywania dowodów elektronicznych po ich przekazaniu organowi wydającemu w celu zapewnienia zgodności z RODO oraz z zasadą przejrzystości[9], jak również z zasadą ograniczonego celu ustanowioną w traktatach o pomocy prawnej.

b) Rezygnacja z zasady podwójnej karalności

EROD uznaje, że wzajemne uznawanie jest uzależnione od stosowania podwójnej karalności, która dla państw członkowskich jest jednym z przejawów ich suwerenności. Podwójna karalność jest jednak postrzegana w coraz większym stopniu jako przeszkoda dla sprawnej współpracy sądowej. Państwa członkowskie UE są coraz bardziej skłonne do współpracy nawet wówczas, gdy środki dochodzeniowe dotyczą czynów, które nie stanowią przestępstwa według ich prawa krajowego. EROD przypomina jednak, że zasada podwójnej karalności służy dodatkowemu zabezpieczeniu tego, aby dane państwo nie mogło zdać się na pomoc innego państwa w zastosowaniu sankcji karnej, której prawo tego innego państwa nie przewiduje. Mogłoby to przykładowo zapobiec sytuacji, w której dane państwo zwraca się o pomoc do innego państwa w celu pozbawienia kogoś wolności za głoszenie określonych poglądów politycznych w sytuacji, gdy ich głoszenie w państwie, do którego się zwrócono o pomoc, nie podlega odpowiedzialności karnej albo w celu ścigania kogoś za dokonanie aborcji w sytuacji, jeżeli osoba ta zamieszkuje w innym państwie, w którym dokonanie aborcji nie jest przestępstwem. Stosowanie zasady podwójnej karalności wiąże się często także z dodatkowymi ograniczeniami lub zabezpieczeniami dotyczącymi sankcji, jeżeli pomiędzy państwem występującym a państwem wykonującym występują bardzo znaczne różnice w ich uregulowaniu. Sztandarowym przykładem jest zobowiązanie się w niektórych traktatach o pomocy prawnej do niestosowania kary śmierci, gdy prawo jednego z państw-stron jej nie przewiduje.

EROD zauważa, że zasada podwójnej karalności nie znalazła się we wniosku dotyczącym rozporządzenia w sprawie dowodów elektronicznych. Oznacza to jednak wyeliminowanie nie tylko zwykłych formalności towarzyszących wzajemnemu uznawaniu, lecz również zabezpieczeń związanych z samą zasadą podwójnej karalności.

EROD zauważa w tym kontekście, że brakuje odesłania do prawa państwa, w którym usługodawca będący adresatem wniosku ma siedzibę, oraz że zabezpieczenie wszelkich danych, jak również wydanie danych abonenta lub danych dostępu, może być przedmiotem nakazu w odniesieniu do wszystkich przestępstw[10], niezależnie od tego, czy inne państwa członkowskie znają podobne rodzaje przestępstw.

Tymczasem nakazy wydania można wydawać i wykonywać jedynie wtedy, gdy podobny środek jest dostępny co do tego samego przestępstwa w porównywalnej sytuacji krajowej w państwie wydającym[11]. Ponadto, jak wyjaśniła Komisja w uzasadnieniu wniosku dotyczącego rozporządzenia, dane dotyczące transakcji i treści mają charakter szczególny, ponieważ uznaje się je za wrażliwsze. Co więcej, nakazy obejmujące dane dotyczące transakcji lub treści wydaje się w oparciu o próg dla przestępstw zagrożonych karą pozbawienia wolności o górnej granicy ustawowego zagrożenia w wysokości co najmniej trzech lat w celu zapewnienia poszanowania zasady proporcjonalności oraz praw osób, których te dane te dotyczą[12]. EROD podkreśla jednak, że nie przeprowadzono jak dotąd na poziomie UE harmonizacji przestępstw zagrożonych karą pozbawienia wolności o górnej granicy ustawowego zagrożenia w wysokości co najmniej trzech lat.

[9] Art. 5 ust. 1 lit. a) RODO.
[10] Art. 5 ust. 3 i art. 6 ust. 2 wniosku dotyczącego rozporządzenia w sprawie dowodów elektronicznych.
[11] Art. 5 ust. 2 wniosku dotyczącego rozporządzenia w sprawie dowodów elektronicznych
[12] Art. 5 ust. 4 lit. a) wniosku dotyczącego rozporządzenia w sprawie dowodów elektronicznych

EROD z dezaprobatą odnosi się do rezygnacji z zasady podwójnej karalności, która ma na celu zapewnienie, aby dane państwo nie mogło zdać się na pomoc innych państw w zastosowaniu jego prawa karnego poza jego terytorium przez państwo, które nie przyjęło takiego samego podejścia, szczególnie biorąc pod uwagę, że nie ma już innych tradycyjnie stosowanych kluczowych zabezpieczeń w dziedzinie prawa karnego (zob. pkt 3 poniżej dotyczący kryteriów terytorialnych oraz pkt 7 lit. g) dotyczący potencjalnych konfliktów z regulacjami prawnymi państw trzecich).

c) Konsekwencje zwracania się bezpośrednio do przedsiębiorstw

EROD dostrzega, że dowody elektroniczne w coraz większym stopniu znajdują się w infrastrukturze prywatnej należącej do dostawców usług oraz że mogą one być dostępne poza granicami państwa prowadzącego dochodzenie lub śledztwo.

EROD zwraca uwagę, że w związku z rozstrzygnięciami w sprawach *Yahoo!*[13] i *Skype*[14] w Belgii oraz w kontekście ataków terrorystycznych zaistniała potrzeba sprawniejszej i szybszej współpracy pomiędzy podmiotami publicznymi a prywatnymi. W ocenie skutków Komisja odnosi się do trzech rodzajów instrumentów proceduralnych angażujących zarówno organy publiczne, jak i dostawców usług. Są to: współpraca sądowa, współpraca bezpośrednia oraz dostęp bezpośredni. O ile ta pierwsza forma nakłada obowiązek wykonania END nie na dostawcę usług, lecz na organ wykonujący[15], druga, tj. współpraca bezpośrednia, opiera się na współdziałaniu dostawcy usług. Z punktu widzenia dostawcy usług najbardziej ingerujący w prywatność jest dostęp bezpośredni, ponieważ organy publiczne mogą uzyskać dostęp do danych bez pomocy podmiotu pośredniczącego.

W związku z powyższym EROD obawia się, że w przypadku kontaktu bezpośredniego dostawcy usług nie zapewnią tak skutecznej ochrony danych osobowych, jaką mogą i są obowiązane zapewnić organy publiczne. EROD podkreśla, że w konsekwencji nie będzie możliwe zastosowanie niektórych gwarancji proceduralnych przewidzianych w ramach współpracy sądowej w odniesieniu do osób fizycznych, jak również do samych przedsiębiorstw[16]. Przykładowo dostawca usług, do którego zwrócono się z wnioskiem, musiałby zaskarżyć nakaz przed sądem innego państwa (członkowskiego), podczas gdy w ramach współpracy sądowej miałby on do czynienia z organami krajowymi. EROD zaleca, aby we wniosku dotyczącym rozporządzenia określone zostały dalsze gwarancje ochrony indywidualnych praw podstawowych, której udzielać będą dostawcy usług. Chodzi tu o ochronę danych osobowych oraz poszanowanie życia prywatnego i rodzinnego. Zalecane jest również informowanie właściwego organu ochrony danych w celu zapewnienia możliwości przeprowadzenia kontroli.

3. Nowa podstawa jurysdykcji oraz tzw. pominięcie kryteriów terytorialnych

EROD zauważa podkreślenie przez Komisję, że jedną z głównych zmian wprowadzonych w przedmiotowych wnioskach jest pominięcie kryteriów terytorialnych i umożliwienie właściwym

[13] Sąd Kasacyjny Belgii, YAHOO! Inc., Nr. P.13.2082.N z dnia 1 grudnia 2015 r.
[14] Sąd karny w Antwerpii, wydział zamiejscowy w Mechelen, Belgia, Nr. ME20.F1.105151-12 z dnia 27 października 2016 r. (Skype odwołał się od tego orzeczenia).
[15] Art. 10–16.
[16] Zob. też w perspektywie międzynarodowej ochrony danych dokument roboczy w sprawie standardów ochrony danych osobowych i prywatności dla transgranicznych wniosków o udostępnienie danych do celów egzekwowania prawa karnego, przyjęty na 63. posiedzeniu Międzynarodowej Grupy Roboczej ds. Ochrony Danych w Telekomunikacji, jakie odbyło się w dniach 9–10 kwietnia 2018 r. w Budapeszcie (Węgry).

organom zwracania się o zabezpieczenie i wydanie danych niezależnie od miejsca ich faktycznego przechowywania.

Z punktu widzenia ochrony danych to żadna nowość, że prawo UE o ochronie danych ma zastosowanie niezależnie od tego, gdzie dane określonych osób są przechowywane. RODO stosuje się bowiem wówczas, gdy administrator lub podmiot przetwarzający mają siedzibę w UE lub gdy przetwarza się dane osobowe osób, których dane dotyczą, przebywających w UE, nawet jeżeli administrator lub podmiot przetwarzający nie mają siedziby w UE[17], w którym to przypadku mają oni obowiązek wyznaczyć przedstawiciela prawnego w UE[18]. Z punktu widzenia ochrony danych należy zauważyć, że ów rozszerzony zakres terytorialny ma na celu zapewnienie pełniejszej ochrony osobom, których dane dotyczą, przebywających w UE, bez względu na to, gdzie przedsiębiorstwo przetwarzające ich dane ma siedzibę.

Dlatego też, mimo że pominięcie kryteriów terytorialnych można potraktować jako nowatorskie w dziedzinie prawa karnego, nie wydaje się, aby stanowiło ono kluczową zmianę z punktu widzenia ochrony danych. Ponadto EROD zauważa również, że powiązanie z terytorium UE występuje nadal, ponieważ wyłącznie dostawcy oferujący usługi w Unii objęci są zakresem omawianych wniosków, a fakt, że wnioski o dane można kierować wyłącznie w ramach postępowania przygotowawczego, oznacza powiązanie z UE (ponieważ przestępstwo popełniono na terytorium państwa członkowskiego albo ofiara przestępstwa lub przestępca był obywatelem państwa członkowskiego).

Skoro kryteria terytorialne nie powinny być już w prawie karnym stosowane, najistotniejsze zdaniem EROD jest to, jak zapewnić, aby niestosowanie tych kryteriów nie wpływało niekorzystnie na ochronę danych, na prawa procesowe osób, których dane dotyczą, i dostawców usług, do których o dane się zwrócono. Z tej perspektywy EROD uznaje, że gwarancje proceduralne w UE zostały, przynajmniej częściowo, zharmonizowane oraz że muszą być one zapewnione zgodnie z europejską konwencją praw człowieka. W związku z tym można stwierdzić, że pominięcie kryteriów terytorialnych miałoby prawdopodobnie bardziej ograniczone skutki, gdyby o dowody zwracano się na terytorium UE w porównaniu z sytuacją odwrotną, w której organy państw trzecich zwracają się o dane do przedsiębiorstw mających siedzibę w UE na tych samych warunkach określonych we wniosku dotyczącym rozporządzenia w sprawie dowodów elektronicznych. W szczególności EROD wyraża obawę, że pominięcie kryteriów terytorialnych może wywołać większą liczbę przypadków problematycznych. W ten sposób bowiem organy państw trzecich, w których w prawie karnym stosuje się różne i potencjalnie słabsze zabezpieczenia proceduralne, mogą mieć dostęp do danych, które w UE byłyby chronione dzięki dodatkowym zabezpieczeniom. Mając to na uwadze, EROD ponownie wyraża obawy co do stosowania podwójnego standardu i osłabiania praw podstawowych w sytuacji, gdy dostawcy usług i osoby, których te dane dotyczą, nie korzystają z zabezpieczeń proceduralnych przewidzianych w prawie UE, jeżeli o dane wystąpił organ państwa trzeciego.

Ponadto, jako że ta nowa podstawa jurysdykcji „niezależna od miejsca, w którym znajdują się dane", powiązana jest z procedurą opartą przede wszystkim na zwracaniu się właściwych organów o dane bezpośrednio do dostawców usług, EROD wyraża obawę, że przedsiębiorstwa prywatne otrzymujące wnioski, które nie są związane instrumentem prawnym, takim jak traktat o pomocy prawnej (tradycyjnie regulujący wymianę danych między organami sądowymi i przewidujący odpowiednie zabezpieczenia służące ochronie danych), tych zabezpieczeń mogą nie stosować. W szczególności w odniesieniu do traktatów o pomocy prawnej stosowanie minimalnych zabezpieczeń ochrony danych

[17] Zob. art. 3, w szczególności ust. 2.
[18] Zob. art. 27

wiąże się np. z obowiązkami zachowania poufności oraz respektowaniem zasady ograniczonego celu, która stanowi, że dane nie będą przetwarzane w innym celu.

EROD przypomina w związku z tym, że należy zapewnić stosowanie zabezpieczeń przewidzianych w dyrektywie 2016/680, w tym tych dotyczących przekazywania danych, a w szczególności przepisów art. 39, w sytuacjach, w których dostawca usług ma siedzibę w państwie trzecim, bez konieczności przyjmowania decyzji stwierdzającej odpowiedni stopień ochrony w tej dziedzinie. EROD podkreśla w szczególności, że przepis ten wymaga między innymi poinformowania właściwego organu ochrony danych w państwie członkowskim organu wydającego nakaz (y) oraz udokumentowania przekazania danych, w tym uzasadnienia bezskuteczności lub nieodpowiedniości przekazania danych do właściwego organu państwa trzeciego.

4. Pojęcie „dostawca usług" należy ograniczyć lub uzupełnić dodatkowymi zabezpieczeniami praw osób, których te dane dotyczą

Jeżeli chodzi o dostawców usług, EROD z zadowoleniem przyjmuje szeroką definicję, która pozwala uwzględnić zarówno usługi komunikacyjne, jak i usługi OTT, ponieważ wszystkie te usługi są funkcjonalnie równoważne, a zatem przewidywane środki mogłyby mieć podobny wpływ na prawo do prywatności i prawo do zachowania tajemnicy komunikowania się, jak podkreślono w oświadczeniu Grupy Roboczej Art. 29 i uprzednio już w opinii 01/2017 w sprawie wniosku dotyczącego rozporządzenia w sprawie prywatności i łączności elektronicznej. I tak, wniosek dotyczący rozporządzenia w sprawie dowodów elektronicznych obejmuje dostawców usług świadczących usługi łączności elektronicznej zdefiniowane w art. 2 ust. 4 dyrektywy ustanawiającej Europejski kodeks łączności elektronicznej, usługi społeczeństwa informacyjnego zgodnie z definicją zawartą w art. 1 ust. 1 lit. b) dyrektywy (UE) 2015/1535, w przypadku których przechowywanie danych jest elementem definiującym usługę świadczoną na rzecz użytkownika, w tym portale społecznościowe, rynki internetowe ułatwiające transakcje pomiędzy użytkownikami oraz inni dostawcy usług hostingowych lub usługi dotyczące nazw domen internetowych i numeracji IP, takie jak dostawcy adresów IP, rejestry nazw domen, podmioty rejestrujące nazwy domen i powiązane usługi prywatności i usługi proxy[19].

Dostawca usług w rozumieniu projektu rozporządzenia to jednak każda osoba fizyczna lub prawna, która świadczy przynajmniej jedną z następujących kategorii usług. EROD wyraża zaniepokojenie tym, że instrument ten mógłby obejmować zarówno administratorów, jak i podmioty przetwarzające dane w rozumieniu RODO. Ponieważ „oferowanie usług", zdefiniowane w art. 2 ust. 4 projektu rozporządzenia, obejmuje zarówno umożliwianie osobom prawnym lub fizycznym w co najmniej jednym państwie członkowskim korzystania z wymienionych usług, jak i posiadanie istotnego powiązania z danym państwem członkowskim lub danymi państwami członkowskimi, czynności te obejmują m.in. czynności wykonywane przez podmiot przetwarzający dane na rzecz administratora danych, takie jak np. przechowywanie danych.

EROD wyraża zatem obawę, że bez nałożenia na dostawców usług działających w charakterze administratorów danych w rozumieniu RODO ograniczeń oraz bez nałożenia szczególnego obowiązku powiadamiania przez podmiot przetwarzający administratora danych o otrzymaniu nakazu wydania lub nakazu zabezpieczenia danych, prawa osób, których te dane dotyczą, mogą nie być respektowane.

[19] Art. 2 ust. 3 lit. c) wniosku dotyczącego rozporządzenia w sprawie dowodów elektronicznych

Właśnie taka sytuacja zachodzi, ponieważ w przypadku ewentualnych sprzecznych zobowiązań uniemożliwiających adresatowi zastosowanie się do otrzymanych nakazów, projekt rozporządzenia zachęca organy sądowe, by kierować nakazy do najbardziej właściwego podmiotu, niezależnie od obowiązujących przepisów dotyczących ochrony danych, w szczególności ze względu na fakt, że zwracać się mogą o wszelkie dane, a nie tylko dane osobowe objęte RODO[20].

Zgodnie z RODO podmiot przetwarzający podejmuje czynności wyłącznie na polecenie administratora. Dlatego obowiązkiem administratora jest zapewnienie przestrzegania praw osób, których dane dotyczą, oraz przekazywanie im odpowiednich informacji, w tym o odbiorcach ich danych, np. w kontekście korzystania z przysługującego im prawa dostępu. Podmiot przetwarzający nie będzie otrzymywał tych wniosków od osób, których dane dotyczą, i nie będzie mógł udzielać odpowiedzi, chyba że administrator wyraźnie się o to zwróci.

W związku z tym, chyba że ich prawo do bycia objętym RODO zostało ograniczone na mocy RODO, EROD podkreśla, że osoby, których dane dotyczą, objęte RODO mogą nie mieć możliwości skutecznego korzystania z przysługujących im praw, jeżeli administrator nie jest w stanie przekazać pełnych informacji. EROD zauważa również, że ryzyko braku informacji jest nawet wyższe, skoro podmiotów przetwarzających nie zobligowano do informowania administratora danych w sytuacjach, w których dane, o które się zwrócono, odnoszą się do osób, których te dane dotyczą, niekorzystających z ochrony przyznanej przez RODO. W tej sytuacji organy sądowe występujące o dane niekoniecznie będą zobligowane do informowania osób, których dane dotyczą, o ich dalszym przetwarzaniu. EROD wzywa zatem do ograniczenia zakresu do administratorów danych w rozumieniu RODO lub do wprowadzenia przepisu precyzującego, że w przypadku gdy dostawca usług, do którego się zwrócono, nie jest administratorem danych, informuje o tym administratora danych.

5. Pojęcia „siedziba" i „przedstawiciel prawny" w kontekście przedmiotowych wniosków powinny być wyraźnie rozróżnione od tych pojęć w ujęciu RODO

Ze względu na niestosowanie kryteriów terytorialnych w odniesieniu do danych adresatami nakazów wydania i nakazów zabezpieczenia są zgodnie z projektem rozporządzenia wyłącznie dostawcy usług oferujący usługi w Unii, niezależnie od tego, czy mają oni siedzibę na terytorium UE. Zgodnie z zasadami określonymi w projekcie dyrektywy dostawcy ci mają obowiązek wyznaczenia przedstawiciela prawnego. Pojęcia „siedziba" i „przedstawiciel prawny" zdefiniowano w związku z tym w projektowanych instrumentach.

EROD zwraca uwagę, że pojęcia te pojawiają się również w kontekście innych instrumentów UE, w szczególności w kontekście RODO. Należy zatem doprecyzować definicje oraz przeprowadzić rozróżnienie tych pojęć w kontekście projektowanych wniosków i w kontekście RODO.

a) Zakład

EROD przypomina również, że pojęcie „zakład" stosowane w kontekście projektu rozporządzenia nie powinno być mylone z tym stosowanym w kontekście RODO. Na potrzeby projektu rozporządzenia pojęcie zakładu zdefiniowane w art. 2 ust. 5 jest szersze niż to w RODO, ponieważ obejmuje ono albo rzeczywiste prowadzenie działalności gospodarczej przez nieokreślony czas za pośrednictwem stabilnej

[20] Zob. art. 7 ust. 3 i 4.

infrastruktury, z której świadczy się usługi, albo stabilną infrastrukturę, z której działalność ta jest zarządzana, niezależnie od tego, czy przetwarzanie danych osobowych odbywa się w kontekście działalności tego zakładu. Jeżeli zatem „zakład" w rozumieniu RODO miał bez wątpienia zawierać się w zakresie tego pojęcia, jak zdefiniowano je w projekcie rozporządzenia, to odwrotność w tym względzie raczej nie zachodzi.

Dlatego też EROD przestrzega, że zakłady dostawców usług w rozumieniu projektu rozporządzenia niekoniecznie oznaczają, że warunki stosowania RODO zgodnie z art. 3 ust. 1 są spełnione. W tym kontekście EROD zachęca administratorów i podmioty przetwarzające, aby sprawdzili, czy stosowanie RODO nie wynika z art. 3 ust. 2, co oznaczałoby konieczność wyznaczenia przedstawiciela prawnego w UE oraz brak mechanizmu kompleksowej obsługi.

b) Przedstawiciel prawny

W swoim oświadczeniu Grupa Robocza Art. 29 podkreśliła, że należy unikać wszelkich niejasności pomiędzy obowiązkiem wyznaczenia przedstawiciela prawnego zgodnie z art. 27 RODO a obowiązkiem wyznaczenia przedstawiciela prawnego zgodnie z projektem rozporządzenia w sprawie dowodów elektronicznych.

Na podstawie gotowego już wniosku EROD pragnie o tych zaleceniach przypomnieć, a w szczególności podkreślić, że w jego rozumieniu przedstawiciel prawny, o którym mowa w projekcie dyrektywy w sprawie mianowania przedstawicieli prawnych w kontekście wniosków dotyczących dowodów elektronicznych, powinien być wyznaczany w każdym przypadku. Należy wyposażyć go w określone funkcje, status niezależny od dostawcy usług, który mu udzielił mandatu, uprawnienie do udzielania odpowiedzi na wnioski i dokonywania czynności w imieniu dostawcy usług, a także określić jego odpowiedzialność w sposób surowszy od odpowiedzialności przedstawiciela prawnego, działającego w reżimie RODO.

Ponadto EROD podkreśla, że pomiędzy RODO a projektowanymi przepisami dotyczącymi dowodów elektronicznych występują różnice, jeśli chodzi o obowiązek wyznaczenia przedstawiciela prawnego, którego zgodnie z projektowanymi przepisami wyznacza się w każdym przypadku niezależnie od tego, czy usługodawca ma siedzibę w UE czy nie, możliwość wyznaczenia nawet kilku przedstawicieli prawnych tego samego dostawcy usług, która to możliwość wynika z projektu dyrektywy dotyczącej dowodów elektronicznych oraz o obowiązek powiadamiania organów państw członkowskich o wyznaczeniu przedstawiciela prawnego, którego to obowiązku RODO nie przewiduje, podobnie jak wyjątków dotyczących wyznaczania i ograniczeń odpowiedzialności przedstawiciela prawnego.

Biorąc zatem pod uwagę istotne różnice pod względem roli, zakresu odpowiedzialności i relacji z innymi zakładami dostawcy usług z jednej strony, a administratora lub podmiotu przetwarzającego z drugiej, EROD zaleca, aby w przypadku gdy dostawca usług nie posiada siedziby na terytorium UE, ale podlega zarówno RODO zgodnie z art. 3 ust. 2, jak i rozporządzeniu w sprawie dowodów elektronicznych, wyznaczonych było dwóch odrębnych przedstawicieli prawnych. Każdy z nich powinien posiadać wyraźnie odrębne funkcje, wynikające z odpowiedniego instrumentu prawnego, na podstawie którego został wyznaczony.

6. Nowe kategorie danych

W projektowanym rozporządzeniu w art. 2 określono różne kategorie danych: dane abonenta, dane dostępu, dane dotyczące transakcji oraz dane dotyczące treści. W motywie 20 wniosku Komisji

stwierdza się, że *kategorie danych objęte zakresem niniejszego rozporządzenia obejmują dane abonenta, dane dostępu, dane dotyczące transakcji (te trzy kategorie danych nazywane są dalej „danymi niedotyczącymi treści") oraz dane dotyczące treści. Powyższe rozróżnienie, nie licząc danych dostępu, istnieje w przepisach prawnych wielu państw członkowskich, a także w obecnym ramach prawnych Stanów Zjednoczonych, umożliwiających usługodawcom dobrowolne udostępnianie danych niedotyczących treści zagranicznym organom ścigania.*

W tym kontekście EROD podkreśla przede wszystkim, że wszystkie cztery kategorie danych, o których mowa powyżej, należy zgodnie z przepisami UE o ochronie danych uznać za dane osobowe, ponieważ zawierają one informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, niezależnie od tego, czy w proponowanym rozporządzeniu osobę, której dane dotyczą, określa się jako „abonenta", czy „użytkownika". Należy również zauważyć, że „dowód elektroniczny" zdefiniowany w art. 2 ust. 6 wniosku Komisji obejmuje wszystkie cztery kategorie danych i w związku z tym odnosi się do danych osobowych. Zamiast zatem ustanawiać zasady dotyczące dostępu do dowodów, definiowanych oraz kwalifikowanych zgodnie z prawem krajowym i procedurami sądowymi, w proponowanym rozporządzeniu przewiduje się nowe materialne i proceduralne warunki dostępu do danych osobowych.

Choć proponowane rozporządzenie ustanawia nowe podkategorie danych osobowych, w odniesieniu do których mają zastosowanie różne proceduralne warunki dostępu, EROD przypomina, że – zgodnie z odpowiednim orzecznictwem Trybunału Sprawiedliwości – dla stwierdzenia sprzeczności z podstawowym prawem do poszanowania życia prywatnego nie ma znaczenia, czy informacja dotycząca życia prywatnego jest wrażliwa lub czy dane osoby doświadczyły jakichkolwiek niedogodności.

Ponadto EROD przypomina, że w odniesieniu do „danych niedotyczących treści" obejmujących dane abonenta, dane dostępu i dane dotyczące transakcji, jak przewiduje wniosek Komisji, Trybunał Sprawiedliwości Unii Europejskiej orzekł w wyroku w sprawach połączonych C-203/15 i C-698/15 Tele *2 Sverige AB*, że metadane, takie jak dane o ruchu i dane dotyczące lokalizacji dają możność ustalenia profilu danych osób, która to informacja jest z punktu widzenia prawa do poszanowania życia prywatnego równie newralgiczna co sama treść komunikatów[21].

Jak już stwierdzono w oświadczeniu Grupy Roboczej Art. 29 w sprawie aspektów ochrony danych i prywatności związanych z transgranicznym dostępem do dowodów elektronicznych z dnia 29 listopada 2017 r., EROD ponownie przedstawia swoje wątpliwości i obawy dotyczące przyjętego rozgraniczenia pomiędzy danymi „niedotyczącymi treści" a danymi dotyczącymi treści oraz czterech kategorii danych osobowych przewidzianych w proponowanym rozporządzeniu. Te cztery proponowane kategorie nie wydają się być jasno wyodrębnione, a definicja „danych dostępu" w porównaniu z innymi kategoriami pozostaje niejasna. EROD wyraża zatem ubolewanie, że ani w ocenie skutków, ani we wniosku Komisja nie przedstawiła szerszego uzasadnienia dla stworzenia tych nowych podkategorii danych osobowych. EROD wyraża również zaniepokojenie ustanowieniem odmiennego poziomu gwarancji związanych z materialnymi i proceduralnymi warunkami dostępu do kategorii danych osobowych, w szczególności uwzględniwszy praktyczne trudności w ocenie, do której kategorii należy zaklasyfikować żądane dane w niektórych przypadkach. Przykładowo adresy IP można przyporządkować zarówno do danych dotyczących transakcji, jak i do danych abonenta.

W tym kontekście EROD przypomina również, że w motywie 14 wniosku dotyczącego rozporządzenia w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej Komisja stwierdza, że „dane pochodzące z łączności elektronicznej należy zdefiniować w dostatecznie szeroki i neutralny technologicznie sposób, aby ich definicja obejmowała wszelkie informacje dotyczące przesyłanych lub przekazywanych treści (treści łączności elektronicznej) oraz informacje dotyczące użytkowników końcowych usług łączności elektronicznej przetwarzane w celu przesyłania, dystrybuowania lub umożliwienia wymiany treści łączności elektronicznej; w tym dane służące do śledzenia i zidentyfikowania źródła i miejsca docelowego przypadku łączności, lokalizacji geograficznej oraz daty, godziny, czasu trwania oraz rodzaju łączności". Ponieważ obecne i przyszłe ramy dotyczące prywatności i łączności elektronicznej, jak również związane z nimi ograniczenia prawa do prywatności, będą miały zastosowanie do przepisów regulujących dostęp organów ścigania do dowodów elektronicznych, EROD zaleca, aby w proponowanym rozporządzeniu rozszerzyć definicję danych pochodzących z łączności elektronicznej w celu zapewnienia odpowiednich zabezpieczeń i warunków dostępu, które spójnie obejmą zarówno „dane niedotyczące treści", jak i „dane dotyczące treści".

7. Analiza procedur europejskiego nakazu wydania dowodów i europejskiego nakazu zabezpieczenia dowodów

Ogólnie rzecz biorąc, wydaje się, że procedura przesyłania nakazów wydania lub zabezpieczenia dowodów wygląda następująco:

- Właściwy organ sądowy – organ wydający – w zależności od rodzaju żądanych danych i od rodzaju nakazu wydaje nakaz zgodnie z (nielicznymi) warunkami wymienionymi w art. 5 i 6, przekazuje nakaz za pośrednictwem zharmonizowanego zaświadczenia do adresata, tj. przedstawiciela prawnego dostawcy usług lub do któregokolwiek z jego zakładów w UE.
- Po otrzymaniu zaświadczenia adresat wykonuje nakaz to znaczy przekazuje dane w terminie 10 dni lub – w sytuacjach wyjątkowych – w terminie 6 godzin lub zabezpiecza je przez okres maksymalnie 60 dni chyba że jest to niemożliwe, ponieważ zaświadczenie jest niekompletne lub zaistniała siła wyższa lub faktyczna niemożliwość dla adresata, lub ponieważ adresat odmawia wykonania nakazu, powołując się na konflikt obowiązków w zakresie praw podstawowych lub podstawowych interesów państwa trzeciego lub na podstawie innych przesłanek.
- Jeżeli adresat nie zastosował się do otrzymanego nakazu bez podania powodów akceptowanych przez organ wydający, przewidziane jest zastosowanie przez właściwy organ przymuszający do wykonania nakazu w państwie członkowskim, w którym dostawca ma swoje przedstawicielstwo lub siedzibę, procedur służących wykonaniu nakazu, chyba że zastosowanie mają ściśle określone przesłanki odmowy, a organ przymuszający sprzeciwił się uznaniu lub wykonaniu nakazu.
- Jeżeli adresat zgłosił uzasadniony sprzeciw wobec nakazu ze względu na konflikt obowiązków, organ wydający kieruje sprawę do właściwego sądu w swoim państwie członkowskim, do którego następnie należy dokonanie oceny potencjalnego konfliktu i utrzymanie nakazu w mocy, o ile stwierdzono brak konfliktu. W razie stwierdzenia konfliktu właściwy sąd albo zwraca się do organów centralnych państwa trzeciego, za pośrednictwem organów centralnych swojego państwa, wyznaczając 15-dniowy termin na odpowiedź (na podstawie uzasadnionego wniosku termin ten może zostać przedłużony do 30 dni) w razie konfliktu obowiązków dotyczącego praw podstawowych lub podstawowych interesów państwa

[21] Wyrok TSUE z dnia 21 grudnia 2016 r., pkt 99.

trzeciego, albo sam rozstrzyga, czy podtrzymać lub wycofać nakaz na podstawie innych przesłanek, na które powołał się adresat.

- Bez uszczerbku dla środków ochrony prawnej na mocy RODO i dyrektywy 2016/680, osoby, których dane uzyskano za pośrednictwem nakazu wydania, mają również prawo do skutecznych środków odwoławczych od tego nakazu.

EROD dokonał oceny procedur i zabezpieczeń przewidzianych w projekcie rozporządzenia, aby oznaczyć poszczególne etapy i po przeanalizowaniu wszystkich aspektów tu przedstawionych zaleca wprowadzenie następujących zabezpieczeń i zmian.

a) Należy podnieść progi powodujące wydanie nakazu, a na wydanie nakazu powinny wydawać zezwolenia sądy

Jeżeli chodzi o warunki wydawania nakazów, EROD z zadowoleniem przyjmuje zasadę stosowania wyższych zabezpieczeń dostępu do danych dotyczących transakcji lub danych dotyczących treści. EROD zauważa jednak, że biorąc pod uwagę brak pełnej harmonizacji sankcji karnych między państwami członkowskimi, odniesienie do przestępstw zagrożonych w państwie wydającym karą pozbawienia wolności o górnej granicy ustawowego zagrożenia w wysokości co najmniej trzech 3 lat[22] nadal oznacza zróżnicowanie progów i powoduje rozbieżności w zakresie ochrony w UE danych osób, których dane dotyczą.

Ponadto EROD podkreśla, że, w szczególności ze względu na szeroką definicję danych abonenta, podany próg wydaje się raczej niski dla nakazów zabezpieczenia i dla nakazów wydania dotyczących danych abonenta lub danych dostępu, ponieważ wszystkie przestępstwa mogą co do zasady uzasadniać wydawanie takich nakazów. Podobnie organy, którym zezwolono na wydawanie takich nakazów, są bardziej ograniczone w kontekście nakazów wydania danych dotyczących transakcji lub danych dotyczących treści, niż w przypadku wydawania nakazów zabezpieczenia lub nakazów wydania dotyczących danych abonenta lub danych dostępu, ponieważ prokuratorzy mogą wystawiać lub zatwierdzać wyłącznie te ostatnie nakazy, podczas gdy każdy sędzia, sąd lub sędzia śledczy może wydać każdy nakaz lub zezwolić na wydanie każdego nakazu.

W szczególności EROD wyraża ubolewanie wobec tego, że najniższy próg umożliwiający organom ścigania wystąpienie o dostęp do danych abonenta i danych dostępu w przypadku każdego przestępstwa opiera się na wykładni *a contrario* orzecznictwa TSUE (który zajmował się innymi danymi) w celu rozróżnienia zabezpieczeń, które mają być ustanowione. Trybunał podkreślił w szczególności, że w przypadku danych o ruchu i danych o lokalizacji, dostęp właściwych organów powinien być ograniczony do celów walki z poważną przestępczością[23]. EROD mógłby uznać to za uzasadnione, jeżeli wniosek przewidywałby możliwość zwrócenia się o dostęp do bardzo podstawowych informacji, które pozwoliłyby tylko na zidentyfikowanie danej osoby bez ujawniania jakichkolwiek danych dotyczących łączności, bez uprzedniej zgody sądu. EROD wyraża jednak dezaprobatę wobec szerokiej wykładni *a contrario* tego orzeczenia przyjętej przez Komisję i wzywa do ustanowienia silniejszych zabezpieczeń w celu ograniczenia podstaw dostępu do innych danych abonenta i danych dostępu. EROD zaleca, aby ograniczyć dostęp do tych danych albo dla przestępstw wymienionych w wykazie zawartym

[22] Zob. art. 5 ust. 3 lit. a)
[23] Zob. sprawa 203/15 – pkt (125)

w projekcie rozporządzenia, albo przynajmniej dla „poważnych przestępstw", w szczególności biorąc pod uwagę niższy próg uprzedniego zezwolenia przewidziany w odniesieniu do tych danych.

Ponadto EROD podkreśla, że taka wykładnia *a contrario* prowadzi również do tego, że wniosek przyznaje prokuratorom możliwość wydawania nakazów lub zezwalania na ich wydawanie. EROD jest zdania, że – z wyjątkiem wniosków o bardzo podstawowe informacje, które pozwoliłyby tylko na zidentyfikowanie danej osoby bez ujawniania jakichkolwiek danych dotyczących łączności – podejście to stanowi krok wstecz w stosunku do orzecznictwa TSUE w zakresie dostępu do danych pochodzących z łączności elektronicznej. W swoim orzecznictwie dotyczącym dostępu do danych pochodzących z łączności elektronicznej do celów egzekwowania prawa TSUE ograniczył możliwość takiego dostępu poprzez uzależnienie go, *z wyjątkiem należycie uzasadnionych pilnych przypadków*[24], między innymi od *uprzedniej kontroli sądu lub niezależnego organu administracyjnego, uzasadnionego wniosku właściwych organów krajowych, złożonego w szczególności w ramach postępowań mających na celu zapobieganie, wykrywanie lub ściganie przestępstw*.[25]

EROD przypomina, że pojęcie „sąd" jest autonomicznym pojęciem prawa UE, oraz że TSUE stale podkreślał i przypominał kryteria, które należy spełnić, aby dany organ zakwalifikować jako sąd, w tym kryterium niezależności,[26] które nie jest spełnione w odniesieniu do prokuratorów, na co wskazał również w swoim orzecznictwie ETPCz[27].

Zatem art. 4 ust. 1) lit. a) i b) oraz art. 3 lit. a) i b) skutkują zastosowaniem procedur zawierających znacząco mniej zabezpieczeń w odniesieniu do danych abonenta i danych dostępu, ponieważ prokurator sam będzie mógł zażądać danych bez dodatkowej kontroli organu państwa, w którym te żądane dane się znajdują lub organu właściwego dla miejsca, w którym będzie znajdował się przedstawiciel prawny przedsiębiorstwa, do którego zwrócono się o dane, ani jakiejkolwiek kontroli niezależnego organu administracyjnego.

Ponadto EROD zwraca uwagę na tzw. dodatkowe zabezpieczenie przewidziane w art. 5 ust. 2, które ogranicza możliwość wydania nakazu wydania danych w przypadku, gdy podobny środek był dostępny w odniesieniu do tego samego przestępstwa w porównywalnej sytuacji krajowej. EROD pragnie jednak ostrzec przed odwrotnymi do zamierzonych skutkami zastosowania takiego przepisu: zamiast wprowadzania dodatkowych zabezpieczeń należy, jak się wydaje, zachęcać państwa członkowskie, aby rozszerzały swoje krajowe opcje zwracania się o wydanie danych abonenta lub danych dostępu i tym samym zapewniały możliwość wydawania nakazów wydania dowodów na podstawie tego rozporządzenia.

b) Terminy udostępniania danych powinny być uzasadnione

EROD zauważa, że na europejski nakaz wydania dowodów należy odpowiedzieć w ciągu 10 dni od daty otrzymania zaświadczenia, chyba że organ wydający wskaże przyczyny uzasadniające wcześniejsze wydanie, zaś w przypadkach nadzwyczajnych, najpóźniej w terminie 6 godzin od daty otrzymania zaświadczenia, zgodnie z art. 9 ust. 1 i 2.

EROD nie doszukał się jednak żadnych kryteriów dotyczących obowiązku wykazywania przez organy, nawet *ex post*, nadzwyczajnego charakteru danej sytuacji wymagającego wydania dowodów, które to kryteria umożliwiłyby kontrolę korzystania z tej bardzo szybkiej procedury ze względu na fakt, że termin sześciogodzinny najprawdopodobniej będzie wiązał się z przeprowadzeniem bardzo

[24] Zob. sprawa 203/15 – pkt (120)
[25] Zob. połączone sprawy C 293/12 i C 594/12 – pkt (62)
[26] Zob. np. sprawa C 203/14
[27] Zob. np. sprawa Moulin przeciwko Francji 23/11/2010

powierzchownej kontroli przed przekazaniem danych, jeżeli nie z brakiem jakiejkolwiek kontroli po stronie dostawcy usług. W ocenie skutków podkreśla się konieczność uzyskiwania przez właściwe organy dostępu do danych w odpowiednim czasie. Wszystkie jednak przytoczone w ocenie skutków przykłady dotyczą dowodów niezbędnych w przypadkach poważnych przestępstw (takich jak ataki terrorystyczne z wzięciem zakładników, trwające wykorzystywanie seksualne dzieci). Uzasadnienie oparte na ulotności dowodów nie wydaje się natomiast być dobrym rozwiązaniem, jeżeli nie mamy do czynienia ze szczególną, pilną koniecznością pozyskania danych, która opiera się na innych podstawach niż ich ulotność. Ponadto ulotność danych nie dostarcza dodatkowej argumentacji, jeżeli chodzi o kryterium proporcjonalności dostępu do danych obwarowanego słabszymi zabezpieczeniami. Dotyczy to sytuacji, w których pozyskanie danych nie jest pilne, a ich zażądanie nie opiera się na innej podstawie niż ich ulotność.

Ponadto EROD wyraża wątpliwość co do konieczności wprowadzenia sześciogodzinnego terminu, przy jednoczesnym założeniu, że nie będzie miał on zastosowania, dopóki organ wydający nie przedstawi dodatkowych wyjaśnień „w terminie pięciu dni" w sytuacji, gdy dostawca usług nie jest w stanie wywiązać się z tego obowiązku.

W związku z tym EROD wzywa do zawarcia w ocenie skutków dodatkowych elementów, które uzasadniałyby niezbędność stosowania tych terminów w przypadkach, gdy popełnione lub ścigane przestępstwo nie jest przestępstwem poważnym oraz- o ile takie szczegółowe elementy nie zostaną przedstawione - do ustanowienia jasnych kryteriów służących uzasadnianiu nadzwyczajnego charakteru sytuacji wtedy, gdy wydawane są zaświadczenia europejskiego nakazu wydania dowodów. Można by przykładowo przedstawić taki sam model, jak zastosowano w dyrektywie END. W dyrektywie END przewidziano krótszy termin, o ile jest to uzasadnione „terminami proceduralnymi, ciężarem przestępstwa lub innymi szczególnie pilnymi okolicznościami (zob. art. 12 ust. 2) lub termin 24-godzinny do podjęcia decyzji co do zastosowania środka tymczasowego (zob. art. 32 ust. 2). Ocena skutków projektu rozporządzenia nie zawiera szczegółowych elementów uzasadniających, dlaczego te terminy nie są efektywne. Jedyne na co wskazano, to znaczna liczba przesyłanych wniosków, których organy sądowe przyjmujące nie są w stanie rozpatrywać w przepisanych terminach.

c) Europejski nakaz wydania dowodów i europejski nakaz zabezpieczenia dowodów można stosować do żądania danych osoby, której te dane dotyczą, z innego państwa członkowskiego jedynie po poinformowaniu właściwych organów tego państwa członkowskiego, w szczególności w odniesieniu do danych dotyczących treści

EROD przypomina, że w ramach obowiązujących instrumentów zapewnia się współpracę sądową i tym samym dodatkowe gwarancje, w szczególności te służące kontroli niezbędności i proporcjonalności wniosków. Należy podkreślić, że stosowanie tych zabezpieczeń jest bardziej uzasadnione wówczas, gdy występuje się o udostępnienie danych dotyczących treści, co wiąże się z większą liczbą ograniczeń praw osób, których dane dotyczą, do ochrony ich danych osobowych i prywatności. W tym względzie EROD przypomina, że w dyrektywie END przewidziano również możliwość przechwytywania przekazów telekomunikacyjnych z pomocą techniczną innego państwa członkowskiego (zob. art. 30), a także obowiązek powiadamiania właściwego organu innego państwa członkowskiego o każdym przechwytywaniu danych, w przypadkach gdy pomoc techniczna nie jest potrzebna do dokonania przechwycenia, a osoba, której dane dotyczą, przebywa lub będzie przebywała na terytorium tego państwa członkowskiego (zob. art. 31).

EROD nie widzi uzasadnienia dla ustanowienia procedury przewidzianej w projekcie rozporządzenia w sprawie dowodów elektronicznych, zakładającej udostępnianie danych dotyczących treści bez

udziału przynajmniej właściwych organów państwa członkowskiego, w którym osoba, której dane dotyczą, przebywa.

d) Europejskie nakazy zabezpieczenia nie mogą być wykorzystywane do obchodzenia obowiązków dostawców usług w zakresie zatrzymywania danych

EROD zauważa, że głównym celem europejskiego nakazu zabezpieczenia jest uniemożliwienie usuwania danych.

Mimo że EROD uznaje, że w niektórych przypadkach wydanie nakazu może być konieczne i proporcjonalne, to wyraża dezaprobatę z powodu braku towarzyszących temu związanych z wydawaniem takich nakazów. W szczególności EROD zaleca, by zagwarantować, że nakaz nigdy nie będzie służył dostawcy danych za podstawę do przetwarzania danych po pierwotnym terminie usunięcia w przypadkach, gdy nakazy zabezpieczenia ograniczają się do danych szczególnych, podczas gdy projekt umożliwia stosowanie nakazów w szerokim zakresie oraz gdy nakazy wydawane są w odniesieniu do danych przeznaczonych do usunięcia zgodnie z zasadą zatrzymywania danych. Innymi słowy, dane powinny być „zamrażane".

Ponadto powiązanie między nakazem zabezpieczenia a późniejszym wnioskiem o wydanie danych, czy to poprzez europejski nakaz wydania, END lub wniosek o wzajemną pomoc prawną, powinno zostać wzmocnione, aby zapewnić wydawanie europejskich nakazów zabezpieczenia tylko wtedy, gdy późniejszy wniosek jest pewny (nie zaś tylko rozważany). Należałoby również zapewnić, aby w przypadku oddalenia tego późniejszego wniosku, upadał również europejski nakaz zabezpieczenia, bez konieczności oczekiwania przez okres 60 dni,[28] jeżeli wniosek oddalono uprzednio.

e) Poufność i informowanie użytkowników

EROD zauważa, że w projekcie rozporządzenia został wprowadzony szczególny artykuł[29] dotyczący poufności przesyłanych nakazów. Aby uniknąć wszelkich niejasności i nieporozumień dotyczących prawa do ochrony danych, EROD przypomina, że choć RODO stanowi, iż ograniczenia praw osób, których dane dotyczą, służące zabezpieczeniu zapobiegania, wykrywania lub ścigania przestępstw, powinny być przewidziane w przepisach prawa, a zatem powinny być publicznie dostępne[30]. Przepisy te powinny wyraźnie wskazywać, że osoby, których dane dotyczą, mają prawo do bycia informowanym o tych ograniczeniach, chyba że może to naruszać cel danego ograniczenia[31]. RODO nie przewiduje jednak obowiązku informowania indywidualnie osób, których dane dotyczą, o każdym wniosku organu ścigania o dostęp do danych.

Tymczasem EROD przypomina jednak, że dyrektywa o ochronie danych nadaje prawo osobie, której dane dotyczą, do bycia informowanym przez same właściwe organy wszystkim osobom, których dane dotyczą, bez ograniczania go tylko do osób mających miejsce zamieszkania na terytorium UE, chyba że prawo to zostało ograniczone.

f) Procedura przymusowego wykonania nakazu w przypadku, gdy dostawca usług odmówił jego wykonania

[28] Zob. art. 10 ust. 1
[29] Zob. art. 11
[30] Zob. art. 23 ust. 1 lit. d)
[31] Zob. art. 23 ust. 2. lit. h)

EROD zauważa, że w art. 14 projektu rozporządzenia przewidziano procedurę mającą na celu zapewnienie przymusowego wykonania nakazu, jeżeli adresat nie zastosował się do niego. Procedura ta opiera się na współpracy sądowej pomiędzy organem wydającym a właściwym organem w państwie wykonującym nakaz.

Wydaje się jednak, że procedura ta nie pozwala organom przymuszającym na odmowę przymusowego wykonania przekazanego nakazu z przyczyn innych niż czysto proceduralne (takie jak przysługujące adresatowi, związane głównie z brakiem wystarczających informacji lub faktyczną niemożnością wydania danych), ponieważ dane te są chronione immunitetem lub przywilejem na podstawie przepisów jego prawa krajowego lub ich ujawnienie może mieć wpływ na podstawowe interesy tego państwa takie jak bezpieczeństwo narodowe i obrona[32].

W związku z tym EROD ponownie wyraża swoje obawy co do niezastosowania, w porównaniu z innymi instrumentami, jakiejkolwiek podwójnej weryfikacji przekazywanego nakazu przez właściwy organ otrzymujący. Nawet odmowa przymusowego wykonania nakazu ze względu na to, że naruszyłoby ono postanowienia Karty wydaje się być mocniejsza aniżeli klasyczne progi związane z naruszeniem praw podstawowych danej osoby. W związku z powyższym, na wzór europejskiego nakazu aresztowania, który przewiduje zarówno obligatoryjne, jak i fakultatywne podstawy odmowy, lub przynajmniej za przykładem dyrektywy END, która ogólnie stanowi, że można obalić domniemanie, zgodnie z którym utworzenie przestrzeni wolności, bezpieczeństwa i sprawiedliwości w Unii opiera się na wzajemnym zaufaniu i domniemaniu przestrzegania przez inne państwa członkowskie prawa Unii, a zwłaszcza praw podstawowych,[33] w projekcie rozporządzenia należy przynajmniej przewidzieć minimalną klasyczną klauzulę derogacyjną, zgodnie z którą, jeżeli zachodzą istotne podstawy do uznania, że przymusowe wykonanie nakazu spowodowałoby naruszenie prawa podstawowego danej osoby, a państwo wykonujące wykazałoby się brakiem poszanowania dla swoich obowiązków związanych z ochroną praw podstawowych zagwarantowanych w Karcie, należy odmówić przymusowego wykonania nakazu.

g) Przymusowe wykonywanie a konflikt obowiązków wynikający z przepisów prawa państwa trzeciego (art. 15–16)

EROD z zadowoleniem przyjmuje przewidzianą w projekcie rozporządzenia możliwość odmowy wykonania nakazu na podstawie tego, że byłoby to sprzeczne z prawami podstawowymi, ponieważ ma ono na celu zapewnienie zabezpieczeń w razie zaistnienia konfliktu obowiązków prawnych. EROD uznaje również za szczególnie ważne, że wniosek przewiduje konsultacje z władzami krajów trzecich, przynajmniej w razie wystąpienia konfliktu, jak również obowiązek uchylenia nakazu, jeżeli organ państwa trzeciego zgłosił sprzeciw.

Należy zatem znacznie ulepszyć procedurę odmowy wykonania nakazu ze względu na konflikt obowiązków wynikający z przepisów prawa państwa trzeciego.

Po pierwsze, EROD zauważa, że w projekcie rozporządzenia powierza się prywatnemu przedsiębiorstwu, jako adresatowi nakazu wydania danych, przeprowadzenie oceny, czy nakaz ten byłby sprzeczny z odnośnymi przepisami prawa państwa trzeciego zakazującymi ujawnienia żądanych danych. Przedsiębiorstwo musi zgłosić uzasadniony sprzeciw, który powinien zawierać wszelkie właściwe informacje na temat przepisów prawa państwa trzeciego, ich stosowalności do danej sprawy oraz charakteru sprzecznych obowiązków.

[32] Zob. art. 14 ust. 2
[33] Zob. motyw 19 dyrektywy END

Co najważniejsze, EROD wyraża zaniepokojenie, że w razie zgłoszenia takiego sprzeciwu właściwy sąd państwa członkowskiego, w którym znajduje się organ wydający, samodzielnie dokona oceny, czy konflikt zachodzi, ponieważ zawiadomi on władze państwa trzeciego dopiero po stwierdzeniu, że konflikt występuje. Dlatego też uprawnienie do ostatecznej wykładni prawa państwa trzeciego w tym względzie należy do właściwego sądu unijnego, który nie do końca jest do rozstrzygania w tej materii powołany. EROD uważa, że obowiązek przeprowadzenia konsultacji z właściwymi organami państwa trzeciego jest zatem w analizowanym wniosku zbyt ograniczony. Jeżeli chodzi o dziedzinę ochrony danych, EROD pragnie zwrócić uwagę prawodawcy na fakt, że w razie dokonania przez właściwy sąd państwa trzeciego wykładni RODO w celu ustalenia, czy jest ono sprzeczne z wymogami tego państwa, unijne organy ochrony danych i właściwe sądy nadal byłyby właściwe w zakresie oceny zgodności z prawem przekazania danych na podstawie orzeczenia sądu lub trybunału lub na podstawie decyzji organu administracyjnego państwa trzeciego nakazującego przekazanie lub ujawnienie danych osobowych w ramach RODO[34].

Ponadto EROD podkreśla, że ocena prawa państwa trzeciego dokonana przez właściwy sąd wnioskującego państwa członkowskiego UE powinna opierać się na przesłankach obiektywnych oraz wiąże się z zastosowaniem kryteriów, które właściwy sąd bierze pod uwagę przy ocenie prawa państwa trzeciego na podstawie art. 15 ust. 4 i art. 16 ust. 5 lit. a) projektu rozporządzenia. Trybunał musiałby ocenić okoliczność, że zamiast mieć na celu ochronę praw podstawowych lub podstawowych interesów państwa trzeciego związanych z bezpieczeństwem narodowym lub obroną, przepisy prawa państwa trzeciego w oczywisty sposób mają na celu ochronę nielegalnych działań przed wnioskami organów ścigania dotyczącymi postępowania przygotowawczego lub interesów chronionych przez właściwe przepisy prawa państwa trzeciego, w tym interesu państwa trzeciego związanego z zapobieżeniem ujawnieniu odnośnych danych. Przykładowo, choć ta ocena w zasadzie powinna wymagać oparcia w dowodach w świetle wszelkich dostępnych informacji, biorąc pod uwagę potencjalny wpływ takiej decyzji, co najmniej sformułowanie w języku angielskim („is being aimed to") wydaje się niejasne i powinno zostać dostosowane („has the aim/objective to").

EROD wyraża ubolewanie, że organy państwa trzeciego byłyby konsultowane i mogłyby wnieść sprzeciw wobec wykonania nakazu wydania wyłącznie wówczas, gdyby ten właściwy sąd unijny uznał, że zachodzi konflikt. Wówczas przekazałby on wszelkie informacje do organów centralnych w zainteresowanym państwie trzecim, a organ centralny tego państwa trzeciego zgłosiłby sprzeciw w maksymalnym ścisłym terminie 50 dni (15 dni, z możliwością przedłużenia o 30 dni, a po upływie ostatniego możliwego ponaglenia – 5 dodatkowych dni). We wszystkich pozostałych przypadkach właściwy sąd mógłby utrzymać w mocy nakaz wydania i nałożyć sankcję pieniężną w przypadku odmowy wykonania nakazu przez dostawcę usług. EROD wyraża w związku z tym obawę, że właściwe sądy unijne nie będą miały szeroko ujętego obowiązku konsultowania się z właściwymi organami zainteresowanych państw trzecich w celu zapewnienia w większym zakresie systematycznego uwzględniania argumentów obu stron oraz uwzględniania i wykazywania jeszcze większego poszanowania dla przepisów prawa państw trzecich.

Zgodnie z powyższym oraz tym, co podkreślono w oświadczeniu Grupy Roboczej Art. 29, EROD przypomina, że szczególną uwagę należy zwrócić na przyjmowanie przez państwa trzecie podobnych instrumentów, które potencjalnie mogą oddziaływać na prawa osób, których dane dotyczą, oraz ich prawo do prywatności w UE, a w szczególności na ryzyko związane z przyjmowaniem instrumentów bezpośrednio kolidujących z unijnym prawem o ochronie danych.

[34] Zob. art. 48 RODO

Ponadto EROD podkreśla, że właściwy sąd państwa członkowskiego organu wydającego może nie być nawet właściwym sądem w zakresie wykonania nakazu na podstawie art. 14 projektu rozporządzenia, co może spowodować wzrost ryzyka wystąpienia kolizji procedur przy braku wzajemnej kontroli sprzecznych ze sobą regulacji prawnych. Wynika to z faktu, że w niektórych przypadkach zaangażowane mogłyby być trzy państwa: państwo organu wydającego nakaz, państwo trzecie dostawcy usług oraz państwo członkowskie, w którym znajduje się przedstawiciel prawny dostawcy usług w UE i w którym nakaz musiałby zostać wykonany. Zgodnie zatem z obecnie przewidzianą procedurą, sąd organu wnioskującego w państwie członkowskim A mógłby dokonać własnej wykładni prawa państwa trzeciego B dostawcy usług, nie zwracając się do organów tego państwa trzeciego o zajęcie stanowiska (które zgłosiłyby sprzeciw wobec tego nakazu) oraz wystąpiłby do sądu innego państwa członkowskiego UE C o wykonanie jego rozstrzygnięcia zupełnie bez możliwości zgłoszenia sprzeciwu.

Ponadto EROD z zadowoleniem przyjmuje wprowadzenie szczególnych środków ochrony prawnej dotyczących nakazów wydania, obok środków przewidzianych w RODO i w dyrektywie 2016/680. Grupa Robocza Art. 29 wezwała do wprowadzenia takich zabezpieczeń w swoim poprzednim oświadczeniu. EROD wyraża jednak ubolewanie z powodu tego, że takie środki ochrony prawnej nie są przewidziane również co do nakazów zabezpieczenia, ponieważ nakazy te mogą również pociągać za sobą ograniczenia praw podstawowych osób fizycznych, których dane zostały zatrzymane. Nakazy zabezpieczenia mogą wywoływać skutek zatrzymania danych przez czas dłuższy aniżeli wystąpiłoby to zgodnie z regulacjami o ochronie danych. W związku z tym nakaz zabezpieczenia danych ze swej istoty powoduje ograniczenie praw podstawowych osoby, której dane dotyczą. Uzasadnienie dla jego wydania podlega kontroli i zastosowaniu szczególnych środków ochrony prawnej, zwłaszcza wówczas, gdy nakaz zabezpieczenia zostanie wydany wraz z nakazem wydania w celu pozyskania danych. Jak zaleciła Grupa Robocza Art. 29 w swoim oświadczeniu, należy przewidzieć środki prawne, co najmniej równoważne środkom dostępnym w sprawie krajowej.

h) Bezpieczne przekazywanie danych w ramach wykonania nakazu

EROD zauważa, że projekt rozporządzenia przewiduje jedynie wydawanie nakazów kierowanych do adresatów w Unii Europejskiej i w związku z tym nie przewiduje szczególnego kanału przekazywania danych pomiędzy adresatami a dostawcami usług zlokalizowanymi poza Unią Europejską.

Choć EROD z zadowoleniem przyjmuje brak dalszych odstępstw od ogólnych ram UE w zakresie ochrony danych, przypomina, że każdy nakaz przesłany do adresata, z którym wiązałoby się przekazanie danych poza UE, musiałby być zgodny z ramami prawnymi ustanowionymi w RODO. Poruszanie się poza ramami prawnymi współpracy sądowej, w których przewidziano obowiązkowe zabezpieczenia ochrony danych, nie powinno jednak prowadzić do obchodzenia przez adresatów nakazów wydania lub nakazów zabezpieczenia wymogów dotyczących przekazywania danych w celu wykonania takich nakazów.

Ponadto, o ile EROD z zadowoleniem przyjmuje brak regulacji zobowiązującej do odszyfrowywania zaszyfrowanych danych[35], to wyraża obawy, że omawiane wnioski nie przewidują szczególnego wymogu dokonywania przez adresatów oceny autentyczności wydawanych danych. EROD podkreśla też, że taka ocena stanowi również wartość dodaną względem tradycyjnych instrumentów opartych na współpracy sądowej i pragnie ostrzec przed zwiększonym ryzykiem dla osób, których dane dotyczą, wynikającym z braku takiej oceny.

[35] Zob. motyw 19 i s. 240 oceny skutków

Podsumowanie

Na podstawie niniejszej analizy EROD pragnie skierować do współprawodawców następujące zalecenia:

1) Podstawą prawną rozporządzenia nie powinien być art. 82 ust. 1 TFUE.
2) Należałoby w większym stopniu uzasadnić niezbędność ustanowienia nowego instrumentu w kontekście obowiązującej dyrektywy END lub traktatów o pomocy prawnej, w tym poprzez dokonanie szczegółowej analizy mniej ingerujących w prawa podstawowe środków, takich jak wprowadzenie zmian w obowiązujących instrumentach lub ograniczenie zakresu tego instrumentu do nakazów zabezpieczenia w połączeniu z innymi dostępnymi obecnie procedurami służącymi występowaniu o dostęp do danych.
3) Rozporządzenie powinno przewidywać dłuższe terminy, aby umożliwić dostawcy usług wykonującemu nakaz przestrzeganie zabezpieczeń służących ochronie praw podstawowych.
4) Należałoby utrzymać zasadę podwójnej karalności, zwłaszcza w związku z rezygnacją ze stosowania kryteriów terytorialnych dotyczących danych w celu utrzymania obowiązku respektowania zabezpieczeń przewidzianych w obu zainteresowanych państwach (tj. w państwie organu wnioskującego i w państwie, w którym dostawca usług się znajduje).
5) Zakres podmiotowy rozporządzenia powinien być ograniczony do administratorów danych w rozumieniu RODO lub należałoby wprowadzić regulację, zgodnie z którą w sytuacji, gdy dostawca usług, do którego się zwrócono, nie jest administratorem danych, lecz podmiotem przetwarzającym, ten ostatni ma obowiązek poinformować administratora danych o wniosku.
6) Rozporządzenie powinno zawierać zabezpieczenia dotyczące przekazywania danych w przypadku, gdyby dostawca usług miał siedzibę w państwie trzecim, dla którego nie wydano decyzji stwierdzającej odpowiedni stopień ochrony w tej dziedzinie, lub odesłanie do dyrektywy 2016/680, ponieważ zabezpieczenia te będą miały zastosowanie.
7) Ponieważ obligatoryjne wyznaczenie przedstawiciela prawnego wykazuje różnice względem rozwiązania przyjętego w RODO, w rozporządzeniu należy sprecyzować, że przedstawiciel prawny wyznaczony na podstawie rozporządzenia w sprawie dowodów elektronicznych nie powinien być utożsamiany z przedstawicielem prawnym wyznaczonym na podstawie art. 3 ust. 2 RODO.
8) Rozporządzenie powinno zawierać szerszą definicję danych pochodzących z komunikacji elektronicznej, aby zapewnić ustanowienie odpowiednich zabezpieczeń i warunków dostępu obejmujących zarówno dane niedotyczące treści, jak i dane dotyczące treści.
9) Rozporządzenie powinno podnieść progi dotyczące wydawania nakazów, które powinny być wydawane lub zatwierdzane przez sądy, z wyjątkiem nakazów dotyczących danych abonenta, pod warunkiem że definicja tej kategorii danych zostanie zasadniczo zawężona do informacji bardzo podstawowych, umożliwiających jedynie identyfikację osoby bez dostępu do jakichkolwiek danych dotyczących łączności.
10) Rozporządzenie powinno ograniczyć dostęp do danych abonenta i danych dostępu dla wniosków dotyczących przestępstw ściśle określonych w odpowiednim wykazie lub co najmniej dotyczących „poważnych przestępstw".
11) W rozporządzeniu należy lepiej uzasadnić termin do wydania danych, zwłaszcza w przypadku sytuacji nadzwyczajnych. Natomiast możliwość stosowania szybkiej sześciogodzinnej procedury powinna wiązać się z obowiązkiem wykazania przez organy wnioskujące, nawet po fakcie, nadzwyczajnego charakteru danej sytuacji powodującego uruchomienie tej procedury w celu umożliwienia kontroli skorzystania z takich wyjątkowych uprawnień.

12) Należy zrezygnować z procedury umożliwiającej wydawanie danych dotyczących treści bez udziału właściwych organów państwa członkowskiego, w którym osoba, której dane dotyczą, się znajduje.
13) W rozporządzeniu należy zawrzeć lepsze zabezpieczenia związane z wydawaniem europejskich nakazów zabezpieczenia.
14) W rozporządzeniu powinna znaleźć się co najmniej minimalna klasyczna klauzula derogacyjna, zgodnie z którą w przypadku, gdy zachodzą istotne podstawy do uznania, że wykonanie nakazu spowodowałoby naruszenie prawa podstawowego danej osoby, wskutek którego państwo wykonujące wykazałoby się brakiem poszanowania dla swoich obowiązków związanych z ochroną praw podstawowych zagwarantowanych w Karcie, należy odmówić przymusowego wykonania nakazu.
15) W rozporządzeniu należy przewidzieć szerszy obowiązek konsultowania się z właściwymi organami państwa trzeciego w przypadku, gdy dostawca usług, do którego zwrócono się o przekazanie danych, znajduje się w sytuacji konfliktu przepisów prawa. Dzięki temu uniknąć można subiektywnej wykładni pochodzącej od pojedynczego sądu.
16) Ważność i termin obowiązywania nakazów zabezpieczenia powinny być w większym stopniu powiązane z towarzyszącymi im nakazami wydania.
17) Należy zapewnić większe bezpieczeństwo przekazywania danych.
18) Należy wprowadzić weryfikację autentyczności danych, w szczególności tam, gdzie mogłyby być dostarczane dane zaszyfrowane.

W imieniu Europejskiej Rady Ochrony Danych

Przewodniczący

(Andrea Jelinek)



Statement on the Digital Services Package and Data Strategy

Adopted on 18 November 2021

The European Data Protection Board has adopted the following statement:

Since November 2020, the European Commission has presented several legislative proposals as part of its digital and data strategies, most notably the Digital Services Act (DSA), the Digital Markets Act (DMA), the Data Governance Act (DGA) and the Regulation on a European approach for Artificial Intelligence (AIR). A fifth proposal for a "Data Act" is expected to be presented very soon, as one of several initiatives announced in the European strategy for Data[1].

The proposals aim to facilitate the further use and sharing of (personal) data between more public and private parties inside 'the data economy', to support the use of specific technologies such as Big Data and AI and to regulate online platforms and gatekeepers. Processing of personal data already is or will be a core activity of the entities, business models and technologies regulated by the proposals. The combined effect of the adoption and implementation of the proposals will therefore significantly impact the protection of the fundamental rights to privacy and to the protection of personal data, enshrined in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union ('the EU Charter') and in Article 16 of the Treaty on the Functioning of the European Union ('TFEU').

The EDPB and EDPS have already issued joint opinions on the DGA[2] and the AIR and the EDPS has issued opinions on the European strategy for Data, on the DMA and on the DSA[3]. These Opinions highlight a number of concerns and make recommendations to bring the proposals more in line with existing Union legislation on data protection. The EDPB regrets that several recommendations have so far not been fully addressed by the co-legislature[4].

[1] Communication from the Commission to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions, A European strategy for data, COM/2020/66 final.
[2] The EDPB has also issued Statement 05/2021 on Data Governance Act in light of the legislative developments.
[3] The EDPS has also issued a Preliminary Opinion on the European Health Data Space. An overview all opinions and statements issues by the EDPB and the EDPS is provided as an annex to this statement.
[4] The concerns highlighted in this Statement concern the initial text of the proposals made by the Commission and do not refer to any subsequent position of the European Parliament or Council of the European Union unless explicitly indicated otherwise.

With this statement, the EDPB draws attention to a number of overarching concerns and urges the co-legislature to take decisive action. Our concerns consist of three categories: (1) lack of protection of individuals' fundamental rights and freedoms; (2) fragmented supervision; and (3) risks of inconsistencies.

The EDPB considers that, without further amendments, the proposals will negatively impact the fundamental rights and freedoms of individuals and lead to significant legal uncertainty that would undermine both the existing and future legal framework. As such, the proposals may fail to create the conditions for innovation and economic growth envisaged by the proposals themselves.

1. LACK OF PROTECTION OF INDIVIDUALS' FUNDAMENTAL RIGHTS AND FREEDOMS

In the proposals, certain choices have been made that are likely to have a long-lasting impact on the fundamental rights and freedoms of individuals and society as a whole. While the proposals seek overall to mitigate a variety of risks, the EDPB holds serious concerns about a number of choices made and considers the fundamental rights and freedoms of individuals require additional protection. Specific examples include:

- The proposal for the AIR would allow for the use of **AI systems categorizing individuals** from biometrics (such as facial recognition) according to **ethnicity, gender, as well as political or sexual orientation**, or other prohibited grounds of discrimination, or AI systems whose scientific validity is not proven or which are in direct conflict with essential values of the EU[5]. The EDPB considers that such systems should be prohibited in the EU and calls on the co-legislators to include such a ban in the AIR. Furthermore, the EDPB considers that the use of AI to **infer emotions of a natural person** is highly undesirable and should be prohibited, except for certain well-specified use-cases, namely for health or research purposes, subject to appropriate safeguards, conditions and limits[6].

- In the same vein, given the significant adverse effect for individuals' fundamental rights and freedoms, the EDPB reiterates that the AIR **should include a ban on any use of AI for an automated recognition of human features in publicly accessible spaces** - such as of faces but also of gait, fingerprints, DNA, voice, keystrokes and other biometric or behavioural signals - in any context.[7] The proposed AIR currently allows for the use of real-time remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement in certain cases[8]. The EDPB welcomes the recently adopted EP Resolution where the significant risks are highlighted[9].

- The EDPB also considers that **online targeted advertising should be regulated more strictly** in the DSA in favour of less intrusive forms of advertising that do not require any tracking of user interaction with content and urges the co-legislature to consider a phase-out leading to a **prohibition of targeted advertising on the basis of pervasive tracking**[10] while the profiling of children should overall be prohibited.

- The EDPB recommends introducing in both the DSA and DMA **interoperability requirements** to promote a digital environment more open to competition, making it easier for individuals to choose among services that offer better privacy and data protection[11].

2. FRAGMENTED SUPERVISION

The proposals all provide for the establishment of supervisory authorities and new European cooperation structures between these authorities ('European Boards')[12]. While the processing of personal data is central to the activities regulated by the proposals, data protection supervisory authorities are not designated as the main competent authorities. The EDPB recalls that, as far as the protection and free flow of personal data is concerned, Article 16(2) TFEU and Article 8(3) of the EU Charter require that the supervision of the processing of personal data be entrusted to independent data protection authorities[13].

Moreover, the EDPB is very concerned that the proposals do not clearly set out how new the supervisory bodies (and the accompanying European Boards) should cooperate with data protection supervisory authorities (and the EDPB). In particular, the proposals fail to adequately address situations of potential overlap in competences or consult each other in matters of mutual concern. This creates a **risk of parallel supervision structures** where different competent authorities supervise the same entities having regard to the same (processing) activities **without structured cooperation** between them.

Specific examples include:

- The proposed DSA requires competent authorities to supervise the **recommender systems**[14] of very large online platforms (which often involve profiling data subjects within the meaning of the GDPR); as well as measures taken to **assess and mitigate systemic risks, including the risk to the right to privacy**[15]. The same proposal also contains provisions on **codes of conduct** that may concern processing of personal data[16]. Yet it does not require competent authorities

[5] E.g., polygraph, Annex III, 6. (b) and 7. (a)) of the AIR. EDPB-EDPS Joint Opinion on the AIR, paragraph 32.
[6] EDPB-EDPS Joint Opinion on the AIR, paragraph 35.
[7] EDPB-EDPS Joint-Opinion on the AIR, paragraph 32.
[8] Specified under Article 5(1)(d)(i)-(iii) AIR.
[9] European Parliament resolution of 6 October 2021 on Artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2016(INI)).

[10] See also the EDPS Opinion on the DSA, paragraphs 69-70, as well as the European Parliament resolution of 20 October 2020 with recommendations to the Commission on a Digital Services Act: adapting commercial and civil law rules for commercial entities operating online (2020/2019(INL)), paragraph 15.
[11] See also EDPS Opinion on the DSA, paragraphs 84-85 and EDPS Opinion on the DMA, paragraphs 37-38.
[12] Digital Markets Advisory Committee (DMAC) in the DMA; European Board for Digital Services (EBDS) in the DSA; European Artificial Intelligence Board (EAIB) in the AIR; European Data Innovation Board (EDIB) in the DGA.
[13] See EDPB statement 05/2021 on the DGA in light of legislative developments, at page 3; the EDPB-EDPS Joint Opinion on the AIR, at page 14.
[14] Article 29 of the DSA.
[15] In particular in the context of Article 27 (identification and assessment of the most prominent and recurrent systemic risks, as well as best practices to mitigate such risks), which refers to Article 26, including 26(1)(b), and Articles 35 and 36 of the DSA (codes of conduct).
[16] See articles 35-36 DSA.

to formally consult or to cooperate with the EDPB or its members. This poses a risk for conflicting guidance or even different outcomes in enforcement actions by supervisory authorities.

- The proposed DGA defines **new types of service providers and organisations** that would process large amounts of potentially sensitive data, notably, data intermediary services and data altruism organisations. However, **the 'vetting' regime for these entities is almost declarative and as such does not provide sufficient protection for data subjects**[17], since it is limited to the verification by the competent authority of (mainly formal) requirements[18] which shall occur within a very short time-limit[19].

- The proposed AIR sets out a **certification scheme and codes of conduct** for high-risk AI systems, but it is unclear if and how these certificates and codes may interface with requirements under the GDPR[20]. This could lead to situations in which AI systems, despite being certified (CE-marked) under the AIR to be placed on the market or put into service, would not be compliant with the rules and principles of data protection (notably, DPbDD)[21]. Furthermore, the proposed AIR lacks any reference to (mandatory) monitoring mechanisms for the codes of conduct designed to verify that providers of non-high-risk AI systems comply with their provisions[22].

- The proposed DMA requires gatekeepers to facilitate the exercise of **data portability** in line with the GDPR and to provide under certain conditions, **access to data**, including personal data, under Article 6(1)(h) and (i) and to anonymised data under Article 6(1)(j), without providing a clear legal basis for the processing of personal data or a duty of consultation and cooperation between any competent authority designated under the DMA with the competent data protection authority when supervising compliance with these provisions of the DMA.

In order to ensure complementarity in oversight and enhance legal certainty, the EDPB strongly recommends that each of the proposals clearly mentions data protection supervisory authorities among the relevant competent authorities with whom cooperation shall take place. In addition, each proposal should **provide for an explicit legal basis for the exchange of information necessary for effective cooperation and identify the circumstances in which cooperation should take place**. Moreover, the proposals should enable the competent supervisory authorities under each proposal **to share information** obtained in the context of any audits and investigations that relate to the processing of personal data with the competent data protection authorities, either upon request or on their own initiative[23]. The EDPB would like to underline the need to ensure that data protection supervisory authorities are provided with **sufficient resources** to perform these additional tasks.

[17] See EDPB EDPS Joint Opinion on the DGA, at paragraphs 136, 140, 151, 155, 175, 180, 191.
[18] Set out, respectively, in Article 11 of the DGA, for data sharing service providers, and Articles 16-19, for data altruism organisations.
[19] One week from the date of notification, for data sharing service providers (Article 10(7) of the DGA); twelve weeks from the date of application for data altruism organizations (Article 17(5) of the DGA).
[20] See EDPB-EDPS Joint Opinion on the AIR, at paragraph 74.
[21] See EDPB-EDPS Joint Opinion on the AIR, at paragraph 76.
[22] See EDPB-EDPS Joint Opinion on the AIR, at paragraph 79.
[23] See also EDPS Opinion on the DSA, at paragraphs 87-89 and EDPS Opinion on the DMA, at paragraphs 39-41.

3. RISKS OF INCONSISTENCIES

The proposals all aim to regulate technologies or activities that involve the processing of personal data. As such, the existing data protection framework is fully applicable. The operative text of the proposals, however, may **create ambiguity** as to the applicability of the data protection framework in certain cases. The co-legislature should resolve any ambiguities **to ensure** legal certainty and enhance coherence with the existing data protection framework in order to ensure its effective application. In any case, the proposals **should clearly state that they shall not affect or undermine the application of existing data protection rules and ensure that data protection rules shall prevail** whenever personal data are being processed[24].

Moreover, some provisions use the same terminology as the GDPR or the ePrivacy Directive, without an explicit reference to the aforementioned legislation. This risks affecting the interpretation given to core concepts of the GDPR (such as the key notion of 'consent' or 'data subject')[25]. It also creates the risk that certain provisions could be read as deviating from the GDPR or the ePrivacy Directive. Consequently, certain provisions **could easily be interpreted in a manner that is inconsistent with the existing legal framework and subsequently lead to legal uncertainty**.

Specific examples include:

- The proposal for a DSA requires service providers to **offer users at least one option for receiving content recommendations that does not involve the use of profiling**.[26] However, the principle of data protection by design and default requires that the systems offering these recommendations should not be based on profiling *by default*[27].

- In many cases, the **legal basis** for processing personal data is not clear from the legal text of the proposals. An example from the proposed DGA is the lack of clarity on the re-use of personal data held by public sector bodies[28]. The proposed AIR indicates that it does not provide a general legal ground for processing of personal data, while at the same time states that the providers of high-risk AI systems "*may process special categories of personal data*" for ensuring bias monitoring, detection and correction and requires additional safeguards for that processing[29].

- **Overlapping terminology** (partly) with clearly different meanings like "online intermediation services" in the proposed DMA and "data intermediation services" in the proposed DGA are confusing and impeding on clarity of the proposals.

- One of the main points of concern regarding the proposed DGA is that the provisions do not sufficiently specify **whether they refer to non-personal data, personal data or both**, nor

[24] In accordance with the fundamental rights to privacy and to the protection of personal data, enshrined in Articles 7 and 8 of the EU Charter and in Article 16 of TFEU.
[25] The EDPB welcomes that in the Council Mandate on the DGA as adopted on 24th of September 2021, the notions of consent and data subject has been brought in line with the requirements for consent in the GDPR.
[26] Article 29 of the DSA.
[27] See EDPS Opinion on the DSA, at paragraph 73.
[28] Article 5(6) of the DGA.
[29] Article 10(5) of the AIR.

specify sufficiently that in case of 'mixed data sets' the GDPR applies. As such, it is not clear that the data protection framework would remain applicable whenever personal data processing takes place, and when specific risks for re-identification of anonymised personal data need to be taken into account.[30] This lack of distinction may lead to confusion, for example, as to whether a legal basis under the GDPR is required (which is the case for all processing of personal data falling within its scope of application)[31].

Looking ahead:

The EDPB is conscious that one of the key initiatives of the European strategy for data is to create **Common European data spaces** in strategic sectors and domains of public interest, including in the area of health ("European Health Data Space"). In the Joint Opinion on the DGA, the EDPB and the EDPS already emphasised that any upcoming initiatives, such as **the Data Act**, that may have an impact on the processing of personal data, must ensure and uphold the respect and application of the EU acquis in the field of personal data protection[32].

At the time of drafting this Statement, the aim and content of the proposals for a Data Act, or for the European Health Data Space are not yet available. However, it is clear that both initiatives will aim to increase access and re-use of (personal) data for the purposes of data sharing between private and public parties.

In a similar vein, the EDPB therefore calls upon the Commission to avoid ambiguities in the new proposals to ensure legal certainty and coherence with the existing data protection framework to ensure its effective application. In any case, the proposals should clearly state that **they shall not affect or undermine the application of existing data protection rules and ensure that data protection rules shall prevail whenever personal data are being processed**[33].

Moreover, mindful of the particular challenges posed by increased data sharing, the EDPB calls for the forthcoming legislative proposals concerning European data spaces and the Data Act to define **specific data protection safeguards** at the outset, ensuring a high level of data protection, taking into account where relevant the processing of special categories of data such as health data. By explicitly defining these safeguards at the outset, we can ensure an adequate level of protection of personal data and avoid potential legal uncertainty.

In addition to the overarching concerns identified above, the EDPB wishes to stress:

(i) the **inalienable nature** of right to the protection of personal data as a right relating to **each natural person**, established under Article 16(1) TFEU and Article 8 of the EU Charter, which cannot be waived[34].

[30] See EDPB EDPS Joint Opinion on the DGA, at page 16.
[31] See further paragraphs 47-56 of the EDPB EDPS Joint Opinion on the DGA pointing out the legal uncertainty regarding the legal basis for the processing of personal data.
[32] EDPB EDPS Joint Opinion on the DGA, paragraph 19.
[33] In accordance with the fundamental rights to privacy and to the protection of personal data, enshrined in Articles 7 and 8 of the EU Charter and in Article 16 of TFEU.
[34] EDPB Statement on the DGA in the light of legislative developments, at page 4.

(ii) the need to incorporate **specific safeguards to ensure compliance with all data protection principles**, in particular **data minimisation, purpose limitation and transparency**. Relevant safeguards include, without being limited to: specifying the types of data which that may be processed, the purposes for which the data may be processed, the data subjects concerned, the parties the personal data may be shared with and storage periods. Particular attention should be paid to the safeguards for processing for the **purposes of scientific research**, ensuring **lawful, responsible and ethical data management**, such as **vetting requirements** for researchers who will have access to large amounts of potentially sensitive personal data[35].

(iii) the importance of the obligation of **data protection by design and by default**, which is particularly relevant in the context of **'connected objects'** (e.g. the Internet of Things and the Internet of Bodies[36]), due to the significant risks to the fundamental rights and freedoms of the persons concerned[37].

For the European Data Protection Board

The Chair

(Andrea Jelinek)

[35] See for example the conditions set out in article 31(4) and 31(5) DSA.
[36] See Inception Impact Assessment to the Data Act, at page 6, referring to "*smart home appliances, wearables and home assistants*", available at: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13045-Data-Act-&-amended-rules-on-the-legal-protection-of-databases_en.
[37] See Article 29 Data Protection Working Party, Opinion 8/2014 on the Recent Development on the Internet of things, p. 6-9, available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf.

ANNEX: List of previous opinions and statements adopted by EDPB and EDPS

- EDPB-EDPS Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act), adopted on 11 March 2021, available at: https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-032021-proposal_en
- EDPB Statement 05/2021 on the Data Governance Act in light of the legislative developments, adopted on 19 May 2021, available at: https://edpb.europa.eu/system/files/2021-05/edpb_statementondga_19052021_en_0.pdf
- EDPB-EDPS Joint Opinion 05/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), adopted on 18 June 2021, available at: https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_en
- EDPS Opinion 01/2021 on the proposal for a Digital Services Act, adopted on 10 February 2021, available at: https://edps.europa.eu/data-protection/our-work/publications/opinions/digital-services-act_en
- EDPS Opinion 02/2021 on the proposal for a Digital Markets Act, adopted on 10 February 2021, available at: https://edps.europa.eu/data-protection/our-work/publications/opinions/digital-services-act_en
- EDPS Opinion 03/2020 on the European strategy for data, adopted on 16 June 2020, available at: https://edps.europa.eu/sites/default/files/publication/20-06-16_opinion_data_strategy_en.pdf
- EDPS Preliminary Opinion 8/2020 on the European Health Data Space, adopted on 17 November 2020, available at https://edps.europa.eu/sites/default/files/publication/20-11-17_preliminary_opinion_european_health_data_space_en.pdf.



Statement 05/2021 on the Data Governance Act in light of the legislative developments

Adopted on 19 May 2021

The European Data Protection Board has adopted the following statement:

On 9 March 2021 the EDPS and the EDPB adopted the Joint Opinion on the Proposal for a Data Governance Act (DGA)[1], which has also been presented at the European Parliament at the hearing of the LIBE Committee of 16 March 2021[2].

The EDPB is closely following the work of the co-legislators on this important legislative initiative, which -we recall- contains provisions concerning the processing of data, including personal data, in the context of the re-use of data held by public sector bodies, of "data sharing services" (which would also include so-called data brokers), and in the context of processing of data (including personal data concerning health) by "data altruism" organizations.

The DGA will have serious impact on the rights and freedoms of individuals and civil society as a whole throughout the EU. In most cases, the processing of personal data would indeed be the core activity of the aforementioned entities[3], and thus on the fundamental rights to privacy and to the protection of personal data, enshrined in Article 7 and 8 of the Charter of Fundamental Rights of the European Union (the Charter), and in Article 16 of the Treaty on the Functioning of the European Union (TFEU). Those rights are a paramount expression of the values of the European Union.

Without robust data protection safeguards, there is a risk that the (trust in the) digital economy would not be sustainable. In other words, data re-use, sharing and availability may generate

[1] EDPB-EDPS Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act), available at : EDPB-EDPS Joint Opinion on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act) | European Data Protection Supervisor (europa.eu)
[2] See the draft agenda of the hearing here.
[3] If not the exclusive activity, in case for instance of providers of data sharing services under letter (b) of Article 9 of the DGA, exclusively referring to personal data.

benefits, but also various types of risk of damages to the persons concerned and society as a whole, impacting individuals from an economic, political and social perspective[4].

To address and mitigate these risks, and to foster individuals trust, data protection principles and safeguards must be implemented from the early design of the data processing, especially when the latter concerns personal data which have not been obtained directly from the natural person/individual concerned. Moreover, the DGA must be consistent not only with the GDPR but also with other Union and national laws, notably the Open Data Directive[5], thus responding to the overarching principle of rule of law, and provide legal certainty for public administrations, legal persons and individuals concerned.

The explanatory memorandum of the DGA states, *"the interplay with the legislation on personal data is particularly important. With the General Data Protection Regulation (GDPR) and ePrivacy Directive, the EU has put in place a solid and trusted legal framework for the protection of personal data and a standard for the world."*[6]

Ensuring consistency between the DGA and the EU data protection acquis

However, as highlighted in the Joint Opinion, **the DGA entails several significant inconsistencies with the GDPR, notwithstanding the statement in the recital that it is "without prejudice" to the GDPR**[7].

The EDPB notes that these inconsistencies have so far not been addressed in the ITRE Draft Report of 26 March 2021[8]. However, the EDPB welcomes that some criticalities raised in the Joint Opinion are addressed in the Council Presidency compromise text of 30 March 2021[9].

To address these inconsistences, we urge the co-legislators to carefully consider[10]:

• First, **the 'interplay' between the DGA and the GDPR** should be clarified under Article 1 of the DGA, considering the GDPR as a regulation providing the 'building blocks' for any solid and trusted legal framework.

• Second, **the definitions/terminology** used in the DGA need integrations and amendments so as to bring them in line with the GDPR.

• Third, **the DGA should clarify without any ambiguity that the processing of personal data shall always be based on an appropriate legal basis under Article 6 of the GDPR**, and also on a specific derogation under Article 9 in case of processing of special categories of personal data.

[4] As an example, in the absence of adequate data protection safeguards, the data collected could be used to build detailed profiles of individuals and used in a way that undermines their interests (e.g. price discrimination or manipulation in the context of electoral campaigns). See at footnote 60 at page 31 of the Joint Opinion, on the risk of use of personal data for unrelated purposes.
[5] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, OJ L 172, 26.6.2019, p. 56.
[6] Explanatory Memorandum, page 1.
[7] See at Section 3.2 of the Joint Opinion.
[8] Available here.
[9] Available here.
[10] See at wection 3.2 of the Joint Opinion, where these critical aspects are recalled at the beginning as points further developed in the Joint Opinion.

• Fourth, as precondition for a clear legal framework, **the provisions of the DGA should specify whether they refer to non-personal data, personal data or both**, and also specify that in case of **'mixed data sets'** the GDPR applies[11].

• Fifth, the constitutional requirement (under Article 16(2) TFEU), according to which **the independent Supervisory Authorities established under the GDPR (the Data Protection Authorities) are 'the' designated authorities competent for the protection of personal data and for the facilitation of the free flow of personal data**, should be mirrored in the DGA.

This means that **Data Protection Authorities must be the main competent authorities in the context of the DGA and inasmuch as personal data is involved,** having regard to public sector bodies, re-users, data sharing service providers, data users, data altruism organizations processing personal data, as well as for the development of guidelines on privacy enhancing technologies (PETs) or on Personal Information Management Systems (PIMS) to foster responsible data innovation.

As recalled in the Joint Opinion[12], "[A]s per their competence and tasks under the GDPR, data protection authorities have already specific expertise in the monitoring of the compliance of data processing, the auditing of specific data processing activities and data sharing, the assessment of the adequate measures to ensure a high level of security for the storage and transmission of personal data, as well as in promoting awareness among controllers and processors of their obligation related to the processing of personal data." Of course, the effective performance of new tasks under the DGA, to be primarily assigned to independent data protection authorities, and to the European Data Protection Board, in compliance with Article 16(2) TFEU, requires the provision of appropriate human, financial, and information technology resources.

The EDPB welcomes in this regard the additional wording in Article 1(3) of the Council compromise text and the specific reference to the powers of the supervisory authorities. For the sake of clarity, and aware of the discretion enjoyed by the co-legislators, the EDPB recommends inserting in the legal text of the DGA (Article 1), the following wording of Article 1(3) of the Council compromise proposal (words in bold added: "**competences and**"):

"*Union and national law on the protection of personal data shall apply to any personal data processed in connection with this Regulation. In particular, this Regulation shall be without prejudice to Regulation (EU) 2016/679 and Directive 2002/58/EC, including the* ***competences and*** *powers of supervisory authorities. In the event of conflict between the provisions of this Regulation and Union law on the protection of personal data, the latter prevails. This Regulation does not create a legal basis for the processing of personal data.*"

The EDPB furthermore calls on the co-legislators to ensure that its overall recommendation in relation to the designated competent authorities and governance at Union level is reflected in the

[11] Where **data sets combine both personal and non-personal data**, the Communication from the Commission to the European Parliament and the Council, *Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union*, COM/2019/250 final, highlights that "if the non-personal data part and the personal data parts are 'inextricably linked', the data protection rights and obligations stemming from the General Data Protection Regulation fully apply to the whole mixed dataset, also when personal data represent only a small part of the dataset."
[12] See para. 153 of the Joint Opinion.

development of their respective positions on the Commission proposal and thus explicitly included in the legal text of the DGA.

In particular, having regard to the definitions laid down in the DGA

The Joint Opinion points out that **the definitions envisaged by the GDPR should apply and they should not be implicitly amended or removed by the DGA, as this would blur the definitions of both these legal frameworks, and thus create legal uncertainty[13].** Furthermore, the new definitions introduced in the DGA, insofar as they relate to the processing of personal data, should not, as a matter of fact, contain 'rules' that are incompatible with the GDPR[14]. This is indeed a crucial point, to which the EDPB would urge the attention of the co-legislators.

On the one hand, the DGA should contain the definitions of 'personal data', 'data subject', 'consent' and 'processing' referring to the definitions in the GDPR[15]; on the other hand, the DGA's definitions of 'metadata', 'data holder', 'data user', 'data sharing', 'data altruism' should be amended to avoid inconsistencies and legal uncertainty, and to be in line with the 'nature of the rights at stake', namely the personal character of the right to the protection of personal data as right relating to each person[16], and as inalienable right, which 'cannot be waived', nor made object of property rights[17].

In this regard, the EDPB regrets the reference to the "exchange, pooling or trade of data" as added in the Council compromise text with regard to the definition of "data sharing service provider", since as far as personal data are concerned, it suggests the idea of legitimizing their trading and is thus inconsistent with the personal character of the right to protection of personal data. Indeed, considering that data protection is a fundamental right guaranteed by Article 8 of the Charter, and taking into account that one of the main purposes of the GDPR is to provide data subjects with control over personal data relating to them, t**he EDPB reiterates that personal data cannot be considered as a "tradeable commodity"**. **An important consequence of this is that, even if the data subject can agree to the processing of his or her personal data, he or she cannot waive his or her fundamental rights[18].** As a further consequence, the controller to whom consent has been provided by the data subject to the processing of her or his personal data is not entitled to 'exchange' or 'trade' personal data (as a so-called 'commodity') in a way that would result as not being in accordance with all applicable data protection principles and rules.

As an example of a provision that might give rise to an interpretation not in line with the aforesaid 'personal character', Article 2(5) of the DGA defines the 'data holder' (including legal persons) as having, among others, the right to grant access to or to share personal data under its control[19]. In this regard, the EDPB remarks that the GDPR guarantees each individual the right to the protection of personal data putting in place a system of checks and balances to protect the individual whenever her or his personal data are processed[20]. The processing of personal data must comply with principles (among which: lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy) and rules, including on data subjects' rights (for instance: the right to information, including about profiling concerning her or him; the right of access; to rectification; to erasure; not to be subject to fully automated decision making significantly affecting her or him) which cannot be waived by the data subject. In this regard, the EDPB notes that, rather to referring to a legal person that "has the right to grant access or to share" personal data, the definition of data holder should, if kept at all, refer to the processing of personal data and the conditions thereof in accordance with applicable data protection law[21].

As specified in the proposed wording for Article 1 DGA, insofar as personal data are concerned, the data protection law prevails (on conflicting rules)[22]. Nevertheless, **it is essential to avoid any conflicting rule or interpretation throughout the text of the regulation, also to improve the prompt readability of the legal text.**

In this sense, a definition of the term 'permission' (by legal entities to the re-use of data) should be introduced to clarify without any ambiguity to what (kind of data) exactly it refers. As stated in the Joint Opinion, we consider that the term should only refer to non-personal data, for the sake of clarity[23].

Concerns related to the sectorial chapters of the DGA

The EDPB also has significant concerns regarding the 'sectorial' Chapters of the DGA (II, III and IV) and wishes to recall some of them hereafter:

• Concerning Chapter II of the DGA, we recall that the Joint Opinion recommends **including in the substantive part of the DGA the specification in recital 7**, namely that "[…] personal data fall outside scope of Directive (EU) 2019/1024 [our note: and fall under the scope of the DGA] insofar as the access regime excludes or restricts access to such data for reasons of privacy and the integrity of the individual, in particular in accordance with data protection rules"[24].

This means that the DGA would apply in particular to the scope carved out of the Open Data Directive pursuant to Article 1(2)(h), that is: *"documents, access to which is excluded or restricted by virtue of the access regimes on grounds of protection of personal data, and parts of documents accessible by*

[13] See at Subsection 3.2.B. of the Joint Opinion.
[14] See para 44 of the Joint Opinion.
[15] See in this regard, Council compromise text of 30 March 2021.
[16] See at para 34 of the Joint Opinion, referring to Article 8 of the Charter: "*1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law.*"
[17] In this regard, at para. 118 of the Joint Opinion: "the clear incentive to 'monetize' personal data also increases the importance on data protection compliance", and footnote 54: "In this regard, the EDPB is developing guidance on the collection and use of personal data against financial remuneration." See also footnote 61, at page 30 of the Joint Opinion.
[18] See EDPB Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects available at: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf

[19] See paras 29-31 of the Joint Opinion. See also the unclear reference to '**their**' data under Article 11(6), Article 19, and 19(1)(a), also highlighted in the Joint Opinion.
[20] See at paras 29 et seq. of the Joint Opinion.
[21] See at para 31 of the Joint Opinion.
[22] In the same sense, see Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, OJ L 136, 22.5.2019, p. 1, Article 3(8): "Union law on the protection of personal data shall apply to any personal data processed in connection with contracts referred to in paragraph 1. In particular, this Directive shall be without prejudice to Regulation (EU) 2016/679 and Directive 2002/58/EC. In the event of conflict between the provisions of this Directive and Union law on the protection of personal data, the latter prevails."
[23] See at para s 47 et seq. of the Joint Opinion.
[24] See at para 69 of the Joint Opinion.

virtue of those regimes which contain personal data the re-use of which has been defined by law as being incompatible with the law concerning the protection of individuals with regard to the processing of personal data or as undermining the protection of privacy and the integrity of the individual, in particular in accordance with Union or national law regarding the protection of personal data". Given the sensitivity of the personal data at stake, to ensure that the level of personal data protection in the EU is not lowered, as well as for legal certainty, the Joint Opinion recommends **aligning Chapter II of the Proposal with the existing rules on the protection of personal data laid down in the GDPR and with the Open Data Directive**. Alternatively, the Joint Opinion invites the co-legislators to consider **excluding personal data** from the scope of this Chapter[25].

In addition, due to the fact that the consent of the data subject might not be considered freely given due to the imbalance of power which is often present in the relationship between the data subject and the public authorities, the Joint Opinion expresses concerns on Article 5(6) of the DGA[26], and, more broadly, invites the co-legislators **to clearly define in the Proposal adequate models of 'civic participation', by which individuals may participate, in an open and collaborative manner, in the process of defining the scenarios allowing the re-use of their personal data, following a bottom-up approach to open data projects.**

The Joint Opinion also recommends **amending the DGA to clarify that the re-use of personal data held by public sector bodies may only be allowed if it is grounded in Union or Member State law** which lays down a list of clear compatible purposes for which the further processing may be lawfully authorised or constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23 of the GDPR[27].

The EDPB further recalls that the inclusion of data held by public sector bodies which are protected on grounds of statistical confidentiality in the scope of Chapter II of the DGA, according to Article 3(1)(b), risks to contradict the principle according to which personal data collected for statistical purpose shall only be used for that purpose[28]. Respect of this principle is key not to undermine trust of the person concerned when she or he provides her or his personal data for statistical purposes[29].

• With regard to Chapter III, **the DGA should specify among the conditions for providing the data sharing service(s), that the provider shall have procedures in place to ensure compliance with the Union and national law on the protection of personal data, including procedures for ensuring the exercise of data subjects' rights**. In particular, the provider shall make available to the data subject easily accessible tools allowing her or him not only to provide but also *to withdraw* consent; and

[25] See at para 71 of the Joint Opinion.
[26] Article 5 (6): "Where the re-use of data cannot be granted in accordance with the obligations laid down in paragraphs 3 to 5 and there is no other legal basis for transmitting the data under Regulation (EU) 2016/679, **the public sector body shall support re-users in seeking consent of the data subjects** and/or permission from the legal entities whose rights and interests may be affected by such re-use, where it is feasible without disproportionate cost for the public sector. In that task they may be assisted by the competent bodies referred to in Article 7 (1)."
[27] See at para 77 of the Joint Opinion. See also paras. 75 and 76 of the Joint Opinion.
[28] See recital 27 of Regulation (EC) No 223/2009 of the European Parliament and of the Council of 11 March 2009 on European statistics; as well as Articles 4 (1) and 4 (2) of the Recommendation of the Council of Europe No R (97)18 concerning the protection of personal data collected and processed for statistical purposes.
[29] See at footnote 36 of the Joint Opinion.

provide tools allowing a comprehensive view of how and for which specific purpose her or his personal data are shared[30].

Moreover, the DGA shall recall the **obligation where applicable to perform a data protection impact assessment pursuant to Article 35 of the GDPR**, and, in case of residual high risks to the persons concerned, to consult the data protection authority prior to the processing in accordance with Article 36 of the GDPR[31].

• **The same requirements should be specified by the DGA in relation to data altruism organizations**[32]. These data protection safeguards must be integrated in the DGA also due to the labelling -as data sharing service provider or as "data altruism organization recognized in the Union"- which would be leveraged by these legal entities to obtain the consent to the processing of her or his personal data by the data subject, who would assume that a high level of protection of such data is ensured.

In light of the above, as noted in the Joint Opinion, **the EDPB considers that the declaratory regime for the notification/registration envisaged respectively by the DGA for data sharing service providers and data altruism organisations does not provide for a sufficiently stringent vetting procedure**, considering the possible impacts for data subjects of the personal data processing that may be undertaken by such entities. Therefore, **the EDPB recommends exploring alternative procedures which should notably take into account a more systematic inclusion of accountability and compliance tools for the processing of personal data as per the GDPR, in particular the adherence to a code of conduct or certification mechanism**[33].

The EDPB regrets that, in the Council compromise text of 30 March 2021, it is now (expressly) provided that the registration as a recognised data altruism organisation is not a precondition for exercising data altruism activities, thus further weakening the checks and safeguards for the data subjects with regard to the crucially important data protection aspects. These safeguards are particularly important also due to the vagueness of the definition of 'data altruism' under the DGA.

Moreover, **the DGA should provide a precise definition of the 'purposes of general interest' that would be pursued by the data altruism organizations**[34]. Besides, the 'European data altruism consent form' for the processing of personal data by data altruism organizations should be developed in consultation with the EDPB, rather than with the (to be established) European Data Innovation Board[35].

• The Joint Opinion noted the requirement of "independence" for data sharing service providers, as well as of "independence" of data altruism organizations in the DGA. Concerning data altruism organizations, the Joint Opinion recommends **clarifying the independence from the for-profit entities of the data altruism organization (e.g. legal, organizational, economical)**[36]. Having regard to data sharing service providers, the EDPB would now like to point out to recital 22 of the DGA: "[..] *Specialised data intermediaries that are independent from both data holders and data users can have*

[30] See at Subsection 3.4.1 and para 147 of the Joint Opinion.
[31] See at para 147 of the Joint Opinion.
[32] See at Subsection 3.5.1 of the Joint Opinion.
[33] See at paras 140 and 180 of the Joint Opinion.
[34] See at paras 159-160 and 170-171 of the Joint Opinion.
[35] See at Subsection 3.5.5 of the Joint Opinion.
[36] See at para. 78 of the Joint Opinion.

a facilitating role in the emergence of new data-driven ecosystems independent from any player with a significant degree of market power. […]" The EDPB underlines that this type of independence of data sharing service providers is key under both the competition and data protection viewpoints[37].

Conclusion

To conclude, the EDPB urges the co-legislators to address the important criticalities explained in the Joint Opinion, thus avoiding that the DGA creates a parallel set of rules, not consistent with the GDPR, as well as with other Union law, which would result in insufficient safeguards for the individuals concerned and difficulties in the practical application.

This statement, recalling some of the key points of the Joint Opinion, is without prejudice to a possible future more detailed statement or opinion on the co-legislators future positions.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

[37] See, in particular: Statement of the EDPB on the data protection impacts of economic concentration, adopted on 27 August 2018, "Increased market concentration in digital markets has the potential to threaten the level of data protection and freedom enjoyed by consumers of digital services"; EDPB Statement on privacy implications of mergers, adopted on 19 February 2020.



Statement 04/2021 on international agreements including transfers

Adopted on 13 April 2021

The European Data Protection Board has adopted the following statement:

As the EDPB/national Supervisory Authorities have been receiving questions about the exchange of personal data between public authorities under existing international agreements in different areas, the EDPB wishes to recall the requirements of Article 96 GDPR and Article 61 Law Enforcement Directive (LED). According to those provisions, all international agreements involving the transfer of personal data to third countries or international organisations which were concluded by the EU Member States prior to 24 May 2016 or 6 May 2016 respectively, and which comply with Union law as applicable prior to that date, shall remain in force until amended, replaced or revoked.

The EDPB deems that, in order to ensure that the level of protection of natural persons guaranteed by the GDPR and the LED is not undermined when personal data is transferred outside the Union, consideration should be given to the aim of bringing these agreements in line with the GDPR and LED requirements for data transfers where this is not yet the case.

The EDPB therefore invites the Member States to assess and, where necessary, review their international agreements that involve international transfers of personal data, such as those relating to taxation (e.g. to the automatic exchange of personal data for tax purposes), social security, mutual legal assistance, police cooperation, etc. which were concluded prior to 24 May 2016 (for the agreements relevant to the GDPR) or 6 May 2016 (for the agreements relevant to the LED). This review should be done in order to determine whether, while pursuing the important public interests covered by the agreements, further alignment with current Union legislation and case law on data protection, as well as EDPB guidance might be needed.

The EDPB recommends that Member States take into account for this review the GDPR and LED themselves, the relevant EDPB guidelines applicable to international transfers, as well as the case-law of the European Court of Justice, including the Schrems II judgment of 16 July 2020[1].

In particular, the EDPB issued Guidelines 2/2020 on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies[2] in December 2020. These guidelines set forth the standard under the GDPR regarding safeguards to be included in legally binding instruments or administrative arrangements between public bodies. The EDPB has also included in its work programme for 2021-2022[3] specific guidance on the safeguards to be included in legally binding instruments pursuant to Article 37(1)(a) LED. National Supervisory Authorities (Article 51 GDPR and Article 41 LED) are available to assist Member States in this process.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

[1]CJEU judgment of 16 July 2020, Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems (C-311/18)
[2]https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202002_art46guidelines_internationaltransferspublicbodies_v2_en.pdf
[3]https://edpb.europa.eu/our-work-tools/our-documents/work-programme/edpb-work-programme-20212022_en



Statement 02/2021 on new draft provisions of the second additional protocol to the Council of Europe Convention on Cybercrime (Budapest Convention)

Adopted on 2 February 2021

The European Data Protection Board has adopted the following statement:

Preliminary remarks and context of the EDPB statement

The European Data Protection Board (EDPB) and data protection authorities within the EU are following closely the development of the second additional protocol to the Budapest Convention and have regularly contributed to the consultation held by the Council of Europe, such as the annual « Octopus conference ». In November 2019, the EDPB also published its latest contribution to the consultation on a draft second additional protocol[1], indicating that it remained « *available for further contributions* » and called for « *an early and more proactive involvement of data protection authorities in the preparation of these specific provisions, in order to ensure an optimal understanding and consideration of data protections safeguards* »[2].

Following up on the publication of new draft provisions of the second additional protocol to the Budapest Convention[3], the EDPB therefore, once again, wishes to provide an expert and constructive contribution with a view to ensure that data protection considerations are duly taken into account in the overall drafting process of the additional protocol, considering that the meetings dedicated to the preparation of the additional protocol are being held in closed sessions and that the direct involvement of data protection authorities in the drafting process has not been foreseen in the T-CY Terms of Reference[4].

[1] https://edpb.europa.eu/sites/edpb/files/files/file1/edpbcontributionbudapestconvention_en.pdf
[2] The EDPB upholds the positions and recommendations expressed in this previous contribution and considers relevant to restate key principles in light of the latest developments and new draft provisions published.
[3] https://www.coe.int/en/web/cybercrime/-/towards-a-protocol-to-the-convention-on-cybercrime-additional-stakeholder-consultations
[4] Terms of Reference for the Preparation of a Draft 2nd Additional Protocol to the Budapest Convention on Cybercrime, Approved by the 17th Plenary of the T-CY on 8 June 2017, T-CY (2017)3.

The EDPB furthermore considers that the abovementioned provisions are likely to affect the substantive and procedural conditions for access to personal data in the EU, including as a result of requests from third country authorities, thus also resonating with ongoing debates at EU level and related legislative initiatives currently being considered by the co-legislators[5]. The EDPB therefore calls on the European Commission and European Parliament, as well as on EU Member States and national Parliaments, to ensure that the ongoing negotiations receive careful scrutiny in order to guarantee the full consistency of the envisaged second additional protocol with the EU acquis, in particular in the field of personal data protection.

Access to personal data across jurisdictions has already been addressed in the past by EU data protection authorities in various positions and opinions and the EDPB wishes to yet again recall in particular the Article 29 Working Party's comments on the issue of direct access by third countries' law enforcement authorities to data stored in another jurisdiction, as proposed in the draft elements for an additional protocol to the Budapest Convention on Cybercrime[6], as well as its statement on data protection and privacy aspects of cross-border access to electronic evidence[7]. The European Data Protection Supervisor has issued Opinion 03/2019 on the mandate for the participation of the Commission in the negotiations[8], as well as Opinion 7/2019 on proposals regarding European Production and Preservation Orders for electronic evidence in criminal matters[9]. These contributions also build upon the EDPB Opinion 23/2018 on Commission proposals on European Production and Preservation Orders for electronic evidence in criminal matters[10].

The EDPB remains fully aware that situations where judicial and law enforcement authorities are faced with a "cross-border situation" with regards to access to personal data as part of their investigations can be a challenging reality and recognises the legitimate objective of enhancing international cooperation on cybercrime and access to information. In parallel, the EDPB reiterates that the protection of personal data and legal certainty must be guaranteed, thus contributing to the objective of establishing sustainable arrangements for the sharing of personal data with third countries for law enforcement purposes, which are fully compatible with the EU Treaties and the Charter of Fundamental Rights of the EU. The EDPB furthermore considers it essential to frame the preparation of the additional protocol within the framework of the Council of Europe core values and principles, and in particular human rights and the rule of law.

With regards to "trans-border direct access to stored computer data" as per Article 32(b) of the Budapest Convention, the EDPB reaffirms in particular that a data controller can normally only disclose data upon prior presentation of a judicial authorisation/warrant or any document justifying the need

[5] In particular, but not exclusively, the discussions on the Commission proposals on European Production and Preservation Orders for electronic evidence in criminal matters.
[6] Article 29 Working Party's comments on the issue of direct access by third countries' law enforcement authorities to data stored in other jurisdiction, as proposed in the draft elements for an additional protocol to the Budapest Convention on Cybercrime, 05/12/2013.
[7] WP29 statement on data protection and privacy aspects of cross-border access to electronic evidence, 29 November 2017.
[8] EDPS opinion 3/2019 regarding the participation in the negotiations in view of a Second Additional Protocol to the Budapest Cybercrime Convention.
[9] EDPS opinion 7/2019 on proposals regarding European Production and Preservation Orders for electronic evidence in criminal matters.
[10] Opinion 23/2018 of the EDPB adopted on 26 September 2018 on Commission proposals on European Production and Preservation Orders for electronic evidence in criminal matters.

to access the data and referring to the relevant legal basis for this access, presented by a national law enforcement authority according to its domestic law that will specify the purpose for which the data is required.

Since the Budapest Convention, as well as any of its additional protocols, are binding international instruments, the EDPB stresses that, in line with the CJEU case law, the "obligations imposed by an international agreement cannot have the effect of prejudicing the constitutional principles of the EC Treaty, which include the principle that all Community acts must respect fundamental rights, that respect constituting a condition of their lawfulness"[11]. It is therefore essential that EU negotiating parties ensure that the provisions laid down in the additional protocol do comply with the EU *acquis* in the field of data protection in order to ensure its compatibility with EU primary and secondary law.

Considering the timeframe of the consultation process, this EDPB contribution will focus on a preliminary assessment of the new draft provisions of the second additional protocol to the Budapest Convention which have not been subject to previous stakeholder consultations:

- Joint investigation teams and joint investigations
- Expedited disclosure of stored computer data in an emergency
- Request for domain name registration information

Once again, the EDPB understands that dedicated provisions on the protection of personal data are still being discussed. The EDPB remains available for further contributions and calls for an early and more proactive involvement of data protection authorities in the preparation of these specific provisions, in order to ensure an optimal understanding and consideration of data protections safeguards.

Provisional draft provisions on joint investigation teams and joint investigations (JITs) (Article 3), on the request for domain name registration information (Article 6) and on expedited disclosure of stored computer data in an emergency (Article 7)

On the basis of its preliminary assessment, the EDPB recommends further examining the provisional draft provisions with regard to the following elements.

The EDPB notes that both the requests for domain name registration information and for expedited disclosure of stored computer data in emergency cases are non-binding requests and grounds for refusal to comply with the request are not clearly defined, while the possibility to rely on the law of the requested State Party to refuse such cooperation, including grounds for refusal set out in MLATs, is also unclear[12]. The EDPB recalls in this regard that the conditions under which the providers of electronic communications services or the entity providing domain name services must grant such access must be provided by law, so as to ensure that the processing relies on a clear legal basis.

[11] See CJEU joined cases C-402/05 P and C-415/05 P, Kadi v. Council, ECLI:EU:C:2008:461 - par (285).
[12] The draft Article 6 (2) refers to "reasonable conditions provided by domestic law" for instance.

The EDPB additionally refers to its previous contribution to reinstate that, except in cases of validly established urgency[13] and, in light of the CJEU case law[14], the EDPB considers that the type of requesting authorities who may issue such request should be limited to a prosecutor, a judicial authority or another independent authority. The EDPB also considers that the systematic involvement of judicial authorities in the requested parties is essential to ensure an effective compliance review of the requests with the Convention and to preserve the application of the principle of double criminality in the field of judicial cooperation.

The EDPB recalls in this regard that the double criminality principle aims at providing an additional safeguard to ensure that a Party cannot rely on the assistance of another to apply a criminal sanction, which does not exist in the law of this other Party. In addition to ensuring respect of individuals' rights and due process in the envisioned mechanism of judicial cooperation, such safeguard also provides for an essential guarantee related to the procedural conditions for access to their personal data. As already mentioned in its previous contribution, in relation to the security of data processing, the EDPB invites the T-CY to consider, as a specific data protection safeguard, a mechanism for the notification without delay of data breaches that could seriously interfere with the rights and freedoms of data subjects. Personal data breaches could indeed potentially have a range of significant adverse effects for individuals concerned.

In relation to the provisional draft provisions on the request for domain name registration information, the EDPB stresses that such information includes personal data and that therefore any international instrument laying down substantive and procedural conditions for accessing such data must, for the Parties members of the European Union, be compliant with EU primary and secondary law.

In relation to the provisional draft provisions on "expedited disclosure of stored computer data in an emergency" (Article 7), the EDPB notes that, depending on its application by each party, this new provision may involve the direct disclosure of content data. The EDPB also notes that the requested State Party may require, after the disclosure of the data, that a proper mutual assistance request is provided (Article 7(5)). In this latter case however, there is no commitment by the Parties to the envisaged Protocol, to delete the data or not to use it as evidence if, on the basis of the supplementary information obtained in the proper mutual assistance request, the requested authorities conclude that the conditions were not met to disclose the data. The legal consequences for the disclosed data, once in the requesting country, seem therefore to be completely left to the discretion of that country's national law. The lack of commitment at the level of the protocol therefore entails the risk to strip this provision of any protecting effect as to the processing of the personal data already disclosed.

The EDPB finally underlines the requirement under Article 52(1) of the Charter of fundamental rights of the EU[15] according to which any limitations to the exercise of the rights and freedoms recognised by the Charter are subject to the principle of proportionality and may only be made if they are necessary. Therefore in order to be lawful under EU law, the draft provisions of the envisaged protocol must fulfil this requirement. It then concerns both the personal data contained in the request as well as in the answer to such a request. **The EDPB is therefore particularly concerned by the wording of the draft Article 6(3) c) and of the draft explanatory report, paragraph 13 in relation to this provision, which seem to imply that requesting third countries Parties to the envisaged Protocol may not be bound to comply with the principle of proportionality when addressing requests to an EU Member State**. In addition, there is not full clarity on the possibility under these provisions to invoke the proportionality principle as a ground for refusal.

It is also unclear whether Parties would be bound by the obligations to ensure, in the context of the envisaged protocol, the conditions and safeguards set out in Article 15 of the Budapest Convention[16]. **The EDPB recommends clarifying that the obligations set forth under Article 15 of the Budapest Convention fully apply also in the context of this cross-border cooperation.**

Provisions on data protection safeguards

The EDPB considers essential that the provisional text made public is complemented by dedicated provisions on data protection safeguards, which must then be assessed together with other provisions, in order to ensure that the draft additional protocol translates into a sustainable arrangement for the sharing of personal data with third countries for law enforcement purposes, fully compatible with the EU Treaties and the Charter of Fundamental Rights.

The provisional draft provisions on request for domain name registration information and expedited disclosure of stored computer data in an emergency, by laying down procedural conditions for access to personal data, may already impact on the level of protection of personal data and may also need to be amended in order to ensure the operational application of appropriate data protection safeguards. **In this regard the EDPB would again like to point out the necessity that the data protection safeguards apply to any exchange of personal data in the context of the envisaged Protocol[17], including in relation to the transfer of personal data[18].**

The EDPB considers that specific provisions on data protection safeguards must reflect key principles and in particular lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality. Likewise, the EDPB would like to stress the importance of ensuring core individual rights (access, rectification, erasure), with any restrictions limited by the principle of proportionality, and of effective judicial redress for data subjects for violations of the data protection safeguards. Exercise of these rights also requires notification of the data subject, at least once this no longer puts at risk the investigation. These principles, rights and obligations are also in line with the modernised Council of Europe Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Convention 108+), to which many Parties to the Budapest Convention on Cybercrime are also Party. In line with Convention 108+, they should apply to all authorities processing the data in the requesting Party, in order to ensure the continuity

[13] The EDPB notes that the notion of emergency is referred to within the meaning of paragraph 1 of the draft provision on Emergency Mutual Assistance and considers that the scope of such situation may be further clarified and framed.
[14] See CJEU joint cases C-203/15 and C-698/15, Tele2 Sverige AB, ECLI:EU:C:2016:970 – par (120)
[15] See also Article 8(2) of the European Convention of Human Rights.

[16] See in particular Article 6(4) in brackets.
[17] Article 6(4) seems to limit the application of the safeguards as well as of Article 15 of the Convention to the information disclosed only and not to the personal data induded in the request.
[18] According to the draft explanatory report, paragraph 9, the latter provision only may/should apply to the transfer of personal data pursuant to the joint investigations teams.

of protection. **The EDPB refers to its contribution in the public consultation in 2019 for further details on the EU requirements in this regard**[19].

The EDPB reiterates the importance of involving data protection authorities in the drafting process of the additional protocol and stands ready to contribute and assist the T-CY in the preparation of provisional text of provisions on data protection safeguards.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

[19] https://edpb.europa.eu/sites/edpb/files/files/file1/edpbcontributionbudapestconvention_en.pdf



Statement on the end of the Brexit transition period

Adopted on 15 December 2020

The European Data Protection Board has adopted the following statement:

- The EDPB wishes to remind all stakeholders that the transition period for the United Kingdom's withdrawal from the European Union will end on 31 December 2020. This means that as of 1 January 2021, the UK will no longer apply the GDPR to the processing of personal data and a separate legal framework regarding data protection and privacy will be in force in the UK.
- The EDPB recalls that, as a consequence, any exchange of personal data between EEA stakeholders and UK entities will constitute a transfer of personal data to a third country and therefore will be subject to the provisions of Chapter V GDPR. In the absence of an adequacy decision applicable to the UK as per Article 45 GDPR, such transfer will require appropriate safeguards as well as enforceable data subject rights and effective legal remedies for data subjects, in accordance with Article 46 GDPR. Subject to specific conditions, it may still be possible to transfer personal data to the UK based on a derogation listed in Article 49 GDPR; however, Article 49 GDPR has an exceptional nature and the derogations it contains must be interpreted restrictively and mainly relate to processing activities that are occasional and non-repetitive. Specific guidance can be found on the EDPB website (https://edpb.europa.eu/our-work-tools/our-documents/other/information-note-data-transfers-under-gdpr-united-kingdom-after_en).
- The EDPB wishes to also recall the consequences regarding the regulatory oversight over ongoing cross-border processing and related complaints, for which the GDPR foresees the One-Stop-Shop (OSS) mechanism. The OSS mechanism envisages that there is one supervisory authority (SA) competent for cross-border processing cases, being the SA of the controller's or processor's main or single establishment in the EEA (the lead supervisory authority), in pursuance of the GDPR.
- As of 1 January 2021, the OSS mechanism will no longer apply to the UK so that the UK Information Commissioner's Office (ICO) will no longer be part of it. The EDPB has been liaising with the ICO over the past months in order to enable a smooth shift to this new situation by ensuring that the EEA authorities follow a shared and efficient approach in handling the existing complaints and cross-border cases involving the ICO, whilst minimizing delays and possible inconveniences to affected complainants.

- The EDPB wishes to emphasize that the decision to benefit from the unified interlocution (the lead supervisory authority) enabled by the OSS mechanism in cross-border processing cases is up to the individual controllers and processors, who to that end may decide whether to set up a new main establishment in the EEA under the terms of Article 4(16) GDPR following the end of the transition period.
- The EDPB recalls in this respect that controllers and processors not established in the EEA but whose processing activities are subject to the application of the GDPR under Article 3(2) GDPR are required to designate a representative in the Union in accordance with Article 27 of the GDPR. The representative may be addressed by supervisory authorities and data subjects on all issues related to processing activities in order to ensure compliance with the GDPR.

For the European Data Protection Board

The Chair

(Andrea Jelinek)



Statement on the protection of personal data processed in relation with the prevention of money laundering and terrorist financing

Adopted on 15 December 2020

The European Data Protection Board has adopted the following statement:

This statement follows the adoption by the European Commission of an Action Plan[1] for a comprehensive Union policy on preventing money laundering and terrorist financing and the launch of a public consultation[2] in May 2020.

According to the Action Plan, the Commission aims to present new legislative proposals in the first quarter of 2021, inter alia, establishing a single rulebook on these topics (i.e. a Regulation or a more detailed revised Directive), ensuring EU level supervision (either by granting new powers to an existing EU Agency or by establishing a new dedicated body), and creating a support and coordination mechanism for Financial Intelligence Units.

The applicable anti-money laundering measures[3] include very broad and far-reaching obligations on financial services providers and other obliged entities to identify and know their customers, to monitor transactions undertaken using their services, and to report any suspicious transactions. Furthermore, the legislation stipulates long retention periods[4]. These measures cover the entire European financial services industry, and therefore affect, in a comprehensive manner, all persons using financial services, each time that they use these services.

[1] Action plan for a comprehensive Union policy on preventing money laundering and terrorism financing, 7 May 2020, available at https://ec.europa.eu/info/publications/200507-anti-money-laundering-terrorism-financing-action-plan_en.
[2] The consultation can be accessed at https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12176-Action-Plan-on-anti-money-laundering/public-consultation.
[3] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, as amended by Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018.
[4] The retention period is the business relationship plus five years (article 40 of Directive (EU) 2015/849). Where the business relationship only covers a single transaction, the retention period is five years. Where there is a long-term business relationship, such as a bank has with its customers, the retention period will often extend over several decennia. Retention periods can be extended by Member States with an additional five years.

The EDPB, and before it the Article 29 Working Party, has repeatedly noted the privacy and data protection challenges related to these measures in the past[5]. The upcoming update to the legislation is an opportunity to address the interplay between the protection of privacy and personal data and the anti-money laundering measures, as well as their concrete application on the ground.

In this context, the EDPB stresses that the intended update to the anti-money laundering framework shall not be undertaken without a review of the relationship between the anti-money laundering measures and the rights to privacy and data protection. In this discussion, relevance and accuracy of the data collected plays a paramount role. The EDPB is indeed convinced that a closer articulation between the two sets of rules would benefit both the protection of personal data and the efficiency of the AML framework. In this respect, the EDPB would like to reiterate the need for a clear legal basis for the processing of personal data and stating the purposes and the limits of such processing, in line with Article 5(1) GDPR, in particular regarding information sharing and international transfers of data, as noted by the EDPS in its opinion on the European Commission's action plan for a comprehensive Union policy on preventing money laundering and terrorism financing[6].

The EDPB considers it as a matter of the utmost importance that the anti-money laundering measures are compatible with the rights to privacy and data protection enshrined in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union, the principles of necessity of such measures in a democratic society and their proportionality, and the case law of the Court of Justice of the European Union.

The EDPB therefore calls on the European Commission to be associated to the drafting process of any new anti-money laundering legislation in its early stages, with a view to provide legal advice on some key points from a data protection perspective, without prejudice to the consultation by the European Commission in line with Article 42 of Regulation 2018/1725 at a later stage. The EDPB is also ready to contribute to discussions within the Council of the EU and the European Parliament during the legislative process.

Going forward, the EDPB stands ready to be involved and consulted in a timely manner by any European or international regulatory bodies or standard-setters, such as the Financial Action Task Force, currently chaired by an EU Member state, before issuance of the revision of their recommendations.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

[5] See for instance Article 29 WP Opinion 14/2011 on data protection issues related to the prevention of money laundering and terrorist financing, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp186_en.pdf.
[6] EDPS Opinion 5/2020 on the European Commission's action plan for a comprehensive Union policy on preventing money laundering and terrorism financing, point 26, 23 July 2020.



Statement on the ePrivacy Regulation and the future role of Supervisory Authorities and the EDPB

Adopted on 19 November 2020

The European Data Protection Board has adopted the following statement:

Firstly, the EDPB wants to stress that this statement is without prejudice to its previous positions, including statement 3/2019[1] and its statement of 25 May 2018[2]. The ePrivacy Regulation must under no circumstances lower the level of protection offered by the current ePrivacy Directive 2002/58/EC, but should complement the GDPR by providing additional strong guarantees for confidentiality and protection of all types of electronic communication.

Secondly, the EDPB welcomes the aim of the Council Presidency to reach a General Approach in order to begin the negotiations with the European Parliament and to adopt the ePrivacy Regulation as soon as possible. However, the EDPB is concerned about some new orientations of the discussions in the Council related to the enforcement of the future ePrivacy Regulation, which would create fragmentation of supervision, procedural complexity, as well as lack of consistency and legal certainty for individuals and companies.

The EDPB recalls that the scope of the proposed Regulation aims at ensuring its uniform application across every Member State and every type of data controller. Any proposed changes in the draft Regulation that may undermine this objective should be avoided to guarantee an equal level playing field for every provider and to ensure the confidentiality of electronic communications, as a fundamental right protected under the Charter, also taking into account the applicable CJEU case law.

In relation to ongoing discussions related to the further processing of electronic communications metadata, the EDPB reiterates its support to the approach of the proposed Regulation, based on broad

[1] European Data Protection Board, Statement 3/2019 on an ePrivacy Regulation, adopted on 13 March 2019, available at:
https://edpb.europa.eu/sites/edpb/files/files/file1/201903_edpb_statement_eprivacyregulation_en.pdf
[2] European Data Protection Board, Statement of the EDPB on the revision of the ePrivacy Regulation and its impact on the protection of individuals with regard to the privacy and confidentiality of their communications, adopted on 25 May 2018, available at:
https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_on_eprivacy_en.pdf

prohibitions, narrow exceptions and the use of consent, while emphasising again that electronic communication metadata can still be processed without consent after it has been genuinely anonymised.

The EDPB also welcomes the inclusion of rules in Article 8 regarding the inclusion of reference to the information covered TV broadcasting services or the software updates, which should be designed in a privacy-friendly way. The EDPB also regrets the lost opportunity to give a clear guidance on the so-called "cookie walls".

Thirdly, the EDPB would like to underline that many provisions of the future ePrivacy Regulation concern processing of personal data. For these processing activities, Article 8(3) of the Charter of Fundamental Rights of the European Union requires oversight by an independent authority. In order to ensure a high level of protection of personal data and to guarantee legal and procedural certainty, this oversight should be entrusted to the same national authorities, which are responsible for enforcement of the GDPR as initially proposed by the European Commission[3]. In its proposal, the European Commission stressed that the cooperation and consistency mechanism foreseen under the GDPR would apply. Moreover, it laid down that all supervisory authorities monitoring the ePrivacy Regulation have to be independent.

Furthermore, in order to guarantee a level playing field on the digital single market, it is essential to ensure a harmonised interpretation and enforcement of the personal data processing elements of the ePrivacy Regulation across the EU. Chapter VII of the GDPR already provides for a well-functioning cooperation and consistency mechanism within the framework of the EDPB: this mechanism should also be used for the supervision of the ePrivacy Regulation in its' personal data protection implications.

It would also benefit data controllers to have a single contact point for all personal data processing operations falling within the scope of ePrivacy Regulation: data controllers would not need to deal with multiple regulatory authorities, which otherwise could lead to diverging standards and interpretations. This does not preclude other authorities concerned from being responsible for parts, which are not related to processing of personal data, while also cooperating with data protection authorities where necessary. The EDPB would also like to recall that there is a clear interconnection of competencies between national authorities competent under the current ePrivacy Directive and data protection authorities[4]. Provisions related to the processing of personal data of the current ePrivacy Directive and the future ePrivacy Regulation should not be applied in isolation, when they are intertwined with personal data processing and the provisions of the GDPR. Consistent interpretation and enforcement of both sets of rules, when covering personal data protection, would therefore be fulfilled in the most efficient way if the enforcement of those parts of the ePrivacy

[3] European Commission, Proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), Brussels, 10 January 2017, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010

[4] European Data Protection Board, Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities, adopted on 12 March 2019, available at: https://edpb.europa.eu/our-work-tools/our-documents/noukogu-arvamus-artikkel-64/opinion-52019-interplay-between-eprivacy_en

Regulation and the GDPR would be entrusted to the same authority. In summary, the future ePrivacy Regulation should be formulated to improve this procedural situation instead of adding complexity.

Moreover, the Council risks creating further procedural uncertainty in case national competent authorities who are not members of the EDPB would have to interact with the EDPB. The future ePrivacy Regulation should lay out a clear framework for the cooperation between data protection authorities as supervisory authorities competent under GDPR and authorities having the appropriate expertise, so their cooperation could function effectively.

Considering the above, the EDPB invites the Member States to support a more effective and consistent ePrivacy Regulation as initially proposed by the European Commission and as amended by the European Parliament.

For the European Data Protection Board

The Chair

(Andrea Jelinek)



Oświadczenie 2/2019 w sprawie wykorzystywania danych osobowych w ramach kampanii politycznych

Przyjęte 13 marca 2019 r.

Europejska Rada Ochrony Danych przyjęła następujące oświadczenie:

Angażowanie wyborców jest nieodłącznym elementem procesu demokratycznego. Pozwala przygotować programy polityczne, umożliwia obywatelom wpływanie na politykę i opracowywanie kampanii zgodnie z oczekiwaniami obywateli.

Partie polityczne, koalicje polityczne i kandydaci w coraz większym stopniu opierają się na danych osobowych i zaawansowanych technikach profilowania w celu monitorowania i kierowania komunikacji do wyborców i osób opiniotwórczych. W praktyce jednostki otrzymują bardzo zindywidualizowane wiadomości i informacje, zwłaszcza na platformach społecznościowych, w oparciu o osobiste zainteresowania, życiowe przyzwyczajenia i wyznawane wartości.

Narzędzia prognostyczne są wykorzystywane do szerokiego klasyfikowania lub profilowania podstawowych cech osobowości, charakteru, nastroju i innych podatności na wpływ, co pozwala na przyjęcie założeń dotyczących głębokich cech osobowości, w tym poglądów politycznych i innych szczególnych kategorii danych. Rozszerzenie takich technik przetwarzania danych na cele polityczne wiąże się z poważnym ryzykiem nie tylko dla prawa do prywatności i ochrony danych, ale również z zaufaniem do uczciwości procesu demokratycznego. Informacje ujawnione w związku ze sprawą Cambridge Analytica pokazują, w jaki sposób potencjalne naruszenie prawa do ochrony danych osobowych może mieć wpływ na inne prawa podstawowe, takie jak wolność wypowiedzi i wolność posiadania poglądów oraz możliwość swobodnego podejmowania decyzji bez manipulacji.

EROD zauważa, że poza partiami politycznymi i kandydatami kilka innych podmiotów może uczestniczyć w przetwarzaniu danych osobowych do celów politycznych: platformy społecznościowe, grupy interesów, brokerzy danych, firmy analityczne, sieci reklamowe. Podmioty te mogą odgrywać ważną rolę w procesie wyborczym, a zgodność ich działania z zasadami podlega nadzorowi niezależnych organów ochrony danych.

W obliczu wyborów do Parlamentu Europejskiego i innych wyborów w UE zaplanowanych na 2019 r. EROD pragnie podkreślić szereg kluczowych kwestii, których należy przestrzegać, gdy partie polityczne przetwarzają dane osobowe w trakcie działań wyborczych:

1. Dane osobowe ujawniające poglądy polityczne zgodnie z RODO są szczególną kategorią danych osobowych. Ogólną zasadą jest, że przetwarzanie takich danych jest zabronione i podlega wielu wąsko interpretowanym warunkom, takim jak wyraźna, świadoma i dobrowolna zgoda osób fizycznych na przetwarzanie danych w konkretnych celach.[1]

2. Dane osobowe, które zostały podane do wiadomości publicznej lub w inny sposób udostępnione przez indywidualnych wyborców, nawet jeśli nie są to dane ujawniające opinie polityczne, nadal podlegają unijnemu prawu o ochronie danych i są przez nie chronione. Na przykład wykorzystywanie danych osobowych zgromadzonych za pośrednictwem mediów społecznościowych nie może odbywać się bez przestrzegania obowiązków dotyczących przejrzystości, określenia celu i zgodności z prawem.

3. Nawet jeżeli przetwarzanie jest zgodne z prawem, organizacje muszą przestrzegać swoich innych obowiązków wynikających z RODO, w tym obowiązku przejrzystości i dostarczania wystarczających informacji osobom, które są badane i których dane osobowe są przetwarzane, czy uzyskano je bezpośrednio lub pośrednio. Partie polityczne i kandydaci muszą być gotowi do wykazania, w jaki sposób przestrzegają zasad ochrony danych, zwłaszcza zasad zgodności z prawem, rzetelności i przejrzystości.

4. Wyłącznie zautomatyzowane podejmowanie decyzji, w tym profilowanie, w przypadku gdy decyzja wywołuje wobec osoby skutki prawne lub w podobny sposób istotnie na nią wpływa, jest ograniczone. Tworzenie profili połączone z przesyłaniem ukierunkowanych komunikatów w ramach kampanii może w pewnych okolicznościach

[1] Zob. art. 9 RODO. Jednym z przykładów jest przetwarzanie danych w sposób oczywisty upublicznionych przez osobę. Podobnie jak inne odstępstwa dotyczące szczególnych kategorii danych, należy go interpretować w sposób zawężający. A zatem nie może być wykorzystany do uzasadnienia przetwarzania danych wywnioskowanych.

"w podobny sposób istotnie" wpływać i co do zasady jest zgodne z prawem wyłącznie za ważną, wyraźną zgodą osoby, której dane dotyczą.[2]

5. Jeżeli chodzi o ukierunkowanie komunikatów, wyborcy powinni otrzymywać odpowiednie informacje wyjaśniające, dlaczego otrzymują konkretną wiadomość, kto jest za nią odpowiedzialny i w jaki sposób mogą oni korzystać z praw przysługujących im jako osobom, których dane dotyczą. Ponadto Rada zauważa, że zgodnie z prawem niektórych państw członkowskich istnieje wymóg przejrzystości w odniesieniu do płatności za reklamę polityczną.

EROD odsyła partie polityczne i pozostałych interesariuszy do praktycznych wytycznych i zaleceń wydanych przez kilka organów ochrony danych dotyczących wykorzystywania danych w trakcie wyborów.[3] Z zadowoleniem przyjmuje również zestaw środków przedstawionych przez Komisję Europejską we wrześniu 2018 r.[4] oraz Konkluzje Rady i państw członkowskich w sprawie zapewnienia wolnych i uczciwych wyborów europejskich.[5]

Członkowie EROD współpracują również z innymi właściwymi organami[6] w celu zapewnienia spójnej interpretacji i przestrzegania obowiązujących przepisów, w tym RODO, w celu zapewnienia zaufania do bezpieczeństwa i uczciwości wyborów do Parlamentu Europejskiego i innych wyborów w UE zaplanowanych na 2019 r. i lata następne.

Przestrzeganie przepisów o ochronie danych, w tym w odniesieniu do działań wyborczych i kampanii politycznych, ma zasadnicze znaczenie dla ochrony demokracji. Jest to również środek służący utrzymaniu zaufania obywateli i uczciwości wyborów. Przed zbliżającymi się terminami wyborów organy ochrony danych są zobowiązane do monitorowania i w razie potrzeby egzekwowania stosowania zasad ochrony danych w kontekście wyborów i kampanii politycznych, takich jak przejrzystość, ograniczenie celu, proporcjonalność i bezpieczeństwo, a także realizację praw osób, których dane dotyczą. Organy ochrony danych będą w pełni

[2] EROD wyjaśniła już wcześniej, że skutek prawny generowany przez automatyczne podejmowanie decyzji może obejmować wpływanie na głosowanie danej osoby.
[3] Zob. załącznik I.
[4] A zwłaszcza Wytyczne dotyczące stosowania prawa UE w zakresie ochrony danych oraz Zalecenie w sprawie sieci współpracy wyborczej, przejrzystości w internecie, ochrony przed cyberincydentami i zwalczania kampanii dezinformacyjnych: https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-cybersecurity-elections-recommendation-5949_en.pdf.
[5] https://data.consilium.europa.eu/doc/document/ST-6573-2019-REV-1/en/pdf. Wersja polska : https://data.consilium.europa.eu/doc/document/ST-6573-2019-REV-1/pl/pdf, https://www.consilium.europa.eu/pl/press/press-releases/2019/02/19/securing-free-and-fair-european-elections-council-adopts-conclusions/
[6] Na przykład w ramach europejskich sieci wyborczych, które zostały opisane bardziej szczegółowo w "pakiecie wyborczym" Komisji [zob. w szczególności Zalecenie w sprawie sieci współpracy wyborczej, o którym mowa w przypisie 4 powyżej, oraz wniosek Komisji dotyczący rozporządzenia Parlamentu Europejskiego i Rady zmieniającego rozporządzenie (UE, Euratom) nr 1141/2014 w odniesieniu do procedury weryfikacji dotyczącej naruszeń przepisów o ochronie danych osobowych w kontekście wyborów do Parlamentu Europejskiego].

korzystały ze swoich uprawnień przewidzianych w RODO oraz zapewnią współpracę i spójność swoich działań w ramach EROD.

W imieniu Europejskiej Rady Ochrony Danych

Przewodnicząca

(Andrea Jelinek)



Annex I to Statement 2/2019 on the use of personal data in the course of political campaigns

Adopted on 13 March 2019

REFERENCES TO GUIDANCE ISSUED BY DATA PROTECTION AUTHORITIES

Belgium

- Guidance from the BE DPA concerning political campaigns/elections:

  NL version: https://www.gegevensbeschermingsautoriteit.be/verkiezingen https://www.gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/Nota_verkiezingen_AVG.pdf

  FR version: https://www.autoriteprotectiondonnees.be/elections https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/Note_elections_RGPD.pdf

EDPS

- EDPS Opinion on online manipulation and personal data: https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf

France

- Communication politique: quelles sont les règles pour l'utilisation des données issues des réseaux sociaux : https://www.cnil.fr/fr/communication-politique-quelles-sont-les-regles-pour-lutilisation-des-donnees-issues-des-reseaux

Greece

- Political Communication Guidance: http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/THEMATIKES_ENOTITES/POLITICAL_COMMUNICATION_DIRECTIONS_V3.0%20FINAL.PDF

Ireland

- Elections and Canvassing: Data Protection and Electronic Marketing: https://www.dataprotection.ie/sites/default/files/uploads/2018-11/Canvassing%20Elected%20Reps%20FINAL.pdf

- Elections & Canvassing: Data Protection and Electronic Marketing – the data protection rights of individuals: https://www.dataprotection.ie/sites/default/files/uploads/2018-11/Canvassing%20-%20Individuals%20update%20final%20version.pdf

Lithuania

- Recommendation on the processing of personal data during elections, prepared by the State Data Protection Inspectorate of the Republic of Lithuania: Rekomendacija dėl asmens duomenų tvarkymo rinkimų metu (2019 m.)

- Press release on the Recomendation: https://www.ada.lt/go.php/lit/Valstybine-duomenu-apsaugos-inspekcija-parenge-rekomendacija-apie-asmens-duomenu-tvarkyma-rinkimu-metu/50

Poland

- Guidelines for political parties and other actors in the electoral process: https://uodo.gov.pl/pl/138/497

Portugal

- Diretriz/2019/1 relativa ao tratamento de dados pessoais no contexto de campanhas eleitorais e marketing político: https://www.cnpd.pt/bin/decisoes/Diretrizes/Diretriz_1_2019_PropagandaPolitica.pdf

Slovenia

- Guidebook for the organisers of election campaigns: http://www.mju.gov.si/fileadmin/mju.gov.si/pageuploads/JAVNA_UPRAVA/Volilna_in_referendumska_zakonodaja/Vodnik_za_organizatorje_volilnih_kampanj_2019.pdf

Spain

- Circular 1/2019, de 7 de marzo, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales relativos a opiniones políticas y envío de propaganda electoral por medios electrónicos o sistemas de mensajería por parte de partidos políticos,

federaciones, coaliciones y agrupaciones de electores al amparo del artículo 58 bis de la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General:
https://www.boe.es/boe/dias/2019/03/11/pdfs/BOE-A-2019-3423.pdf

United Kingdom

- Guidance on political campaigning:
https://ico.org.uk/media/1589/promotion_of_a_political_party.pdf



Statement 01/2019 on the US Foreign Account Tax Compliance Act (FATCA)

The European Data Protection Board has adopted the following statement:

This statement follows the Resolution passed by the European Parliament on 5 July 2018 on the adverse effects of the US Foreign Account Tax Compliance Act (FATCA) on EU citizens[1] and the requests made by the Association of Accidental Americans to the WP29 in this respect.

European Data Protection Authorities have long been attentive to the data protection issues raised by the automatic exchange of personal data for tax purposes. The Article 29 Working Party (WP29), which preceded the European Data Protection Board, has taken several actions in the past with regards to the automatic exchange of personal data for tax purposes and more specifically with regards to the US Foreign Account Tax Compliance Act (FATCA) in two letters published on 21 June 2012[2] and on 1 October 2012[3]. The WP29 also issued a statement on automatic inter-state exchanges of personal data for tax purposes (WP 230 - 4 February 2015) and guidelines for Member States on the criteria to ensure compliance with data protection requirements in the context of the automatic exchange of personal data for tax purposes (WP 234 - 16 December 2015). Finally, the WP29 addressed a letter to the Association of Accidental Americans (8 February 2018)[4] with regards to the scope of application of the FATCA legislation and relevant data protection issues.

With respect to the European Parliament resolution of 5 July 2018, the European Data Protection Board (EDPB) will pay due attention to the call made to it to review the existing data protection safeguards under the legislation authorising the transfer of personal data to the US IRS for the purposes of the US Foreign Account Tax Compliance Act. It however wishes to highlight that it has initiated work on the preparation of guidelines on some of the tools provided for by Article 46 of the GDPR. More specifically, the guidelines will provide information to interested stakeholders on the elaboration of transfer tools based on Articles 46 (2) (a) and 46 (3) (b) of the GDPR.

[1] European Parliament resolution of 5 July 2018 on the adverse effects of the US Foreign Account Tax Compliance Act (FATCA) on EU citizens and in particular 'accidental Americans'
[2] Letter of the Chair of the ART 29 WP to the Director General of Taxation and Customs Union 21 June 2012
[3] Letter of the Chair of the ART 29 WP to the Director General of Taxation and Customs Union 01 October 2012
[4] Letter of the Chair of the ART 29 WP to collective of European "accidental Americans" 08 February 2018

This guidance will include information on the minimum guarantees to be included in legally binding and enforceable instruments concluded between public authorities and bodies (46 (2) (a)) as well as for provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights (46 (3) (b)). It should be noted that legally binding instruments do not require specific authorisation from a supervisory authority whereas the provisions to be included in administrative arrangements are subject to such authorisation from the competent supervisory authority.

This set of guidelines, which should be adopted by the EDPB before the end of 2019, will be a useful tool also for the evaluation of intergovernmental agreements signed between Member States and the US government on FATCA to ensure their compliance with the GDPR.

For the European Data Protection Board

The Chair

(Andrea Jelinek)



Statement of the EDPB on the data protection impacts of economic concentration

EU data protection authorities have noted the Commission's intention to analyse the effects of further concentration of 'commercially sensitive data about customers' personal data in the context of its investigation into the proposed acquisition of Shazam by Apple.[1] We consider it essential to assess longer-term implications for the protection of economic, data protection and consumer rights whenever a significant merger is proposed, particularly in technology sectors of the economy.

Increased market concentration in digital markets has the potential to threaten the level of data protection and freedom enjoyed by consumers of digital services. The data protection and privacy interests of individuals are relevant to any assessment of potential abuse of dominance as well as mergers of companies, which may accumulate or which have accumulated significant informational power.

Independent data protection authorities can help with the assessment of such an impact on the consumer or society more generally in terms of privacy, freedom of expression and choice. This assessment, as well as the identification of conditions or remedies for mitigating negative impacts on privacy and other freedoms, may be separate to and independent from, or integrated into, the analysis carried out by competition authorities during their assessment under competition law.

[1] European Commission - Press release, "Mergers: Commission opens in-depth investigation into Apple's proposed acquisition of Shazam", 23 April 2018, http://europa.eu/rapid/press-release_IP-18-3505_en.htm



Oświadczenie Europejskiej Rady Ochrony Danych dotyczące zmiany rozporządzenia w sprawie prywatności i łączności elektronicznej oraz jego wpływu na ochronę osób fizycznych w zakresie prywatności i poufności komunikacji

Organy ds. ochrony danych Unii Europejskiej, zjednoczone w Europejskiej Radzie Ochrony Danych (EROD), uznają rewizję obowiązującej dyrektywy o prywatności i łączności elektronicznej (2002/58/WE, zmienionej dyrektywą 2009/136/WE) za ważną, konieczną i wymagającą szybkiego zakończenia. Począwszy od 2009 r. bardzo rozpowszechniły się usługi komunikacyjne oparte na IP, znane jako usługi OTT (*over-the-top*), które nie są objęte obowiązującą dyrektywą. Aby zapewnić użytkownikom końcowym ochronę poufności komunikacji przy korzystaniu z tych nowych usług, a także aby stworzyć równe warunki działania dla dostawców łączności elektronicznej i usług funkcjonalnie równoważnych, wzywamy Komisję Europejską, Parlament i Radę do współpracy w celu szybkiego przyjęcia nowego rozporządzenia w sprawie prywatności i łączności elektronicznej („rozporządzenie o e-prywatności"), które powinno zastąpić obecnie obowiązującą dyrektywę jak najszybciej po wejściu w życie ogólnego rozporządzenia o ochronie danych („RODO") w maju tego roku.

Biorąc pod uwagę przebieg prac nad wnioskiem, a także z myślą o współprawodawcach, EROD postanowiła udzielić dalszych porad i wyjaśnień dotyczących pewnych konkretnych kwestii związanych z poprawkami proponowanymi przez współprawodawcę.

1. Poufność komunikacji elektronicznej wymaga szczególnej ochrony wykraczającej poza przepisy RODO.

Poufność komunikacji (nowoczesny odpowiednik tradycyjnej tajemnicy korespondencji) jest prawem podstawowym chronionym na mocy art. 7 Karty praw podstawowych Unii Europejskiej, wdrożonym już dyrektywą o prywatności i łączności elektronicznej. Prawo do zachowania poufności musi być stosowane do każdego rodzaju przekazu elektronicznego, niezależnie od sposobu jego wysłania, czy to w trakcie przesyłu, czy w oczekiwaniu na przesył, na każdym etapie od wysłania do doręczenia. Ochrony wymaga również integralność urządzeń końcowych każdego użytkownika.

Łączność elektroniczna to w naszych nowoczesnych społeczeństwach podstawa działalności w wielu istotnych dziedzinach, wspierająca korzystanie z licznych praw podstawowych – wolności myśli, sumienia, wyznania, wypowiedzi, informacji, zgromadzeń, stowarzyszeń itp. Konieczne jest zatem skuteczniejsze zapewnienie poufnego i neutralnego charakteru usług przekazywania wiadomości.

Biorąc pod uwagę powszechność i znaczenie łączności elektronicznej w naszym życiu cyfrowym, wiadomości elektroniczne niejednokrotnie zawierają lub ujawniają szczególne kategorie danych osobowych, czy to bezpośrednio, czy choćby tylko ze względu na nagromadzenie i połączenie treści i metadanych, co pozwala na wyciąganie bardzo dokładnych wniosków na temat życia prywatnego poszczególnych osób. Wiąże się to z wysokim ryzykiem dla praw i wolności osób i wymaga w związku z tym odpowiedniego podejścia.

Z tego względu w pełni popieramy środki przewidziane w proponowanym rozporządzeniu, polegające na szeroko ujętych zakazach, ograniczonych wyjątkach i wymogu uzyskania zgody. Rozporządzenie o e-prywatności nie powinno zatem zezwalać na przetwarzanie treści i metadanych pochodzących z łączności elektronicznej na ogólnie sformułowanych podstawach, takich jak „prawnie uzasadnione interesy", które wykraczają poza zakres konieczny do świadczenia usługi łączności elektronicznej. Rozporządzenie nie powinno również umożliwiać przetwarzania metadanych pochodzących z łączności elektronicznej do celów wykonania umowy, a więc nie powinno przewidywać wyjątku dotyczącego ogólnie tego celu, ponieważ określa ono już dokładnie, jakie rodzaje przetwarzania są w tym celu dozwolone (np. przetwarzanie do w celu naliczania opłat).

EROD podkreśla, że metadane pochodzące z łączności elektronicznej mogą być nadal przetwarzane bez zgody osoby, której dane dotyczą, pod warunkiem ich rzeczywistej anonimizacji[1]. EROD zachęca dostawców usług łączności elektronicznej do korzystania z tej możliwości w celu tworzenia innowacyjnych usług przy jednoczesnym zachowaniu prywatności.

2. Dyrektywa o prywatności i łączności elektronicznej już obowiązuje.

Ochrona poufności komunikacji to już istniejące prawo. W dyrektywie o prywatności i łączności elektronicznej z 2002 r., zmienionej w 2009 r., ustanowiono już ogólny zakaz przetwarzania treści i metadanych pochodzących z łączności elektronicznej. Działania takie są dopuszczalne wyłącznie:

- za uprzednią zgodą użytkownika, lub
- jeżeli spełniają jeden z wyjątków przewidzianych w dyrektywie o prywatności i łączności elektronicznej (transmisja komunikatu lub naliczanie opłat).

Usługi transmisji wykorzystywane do świadczenia usług w trybie maszyna-maszyna także są objęte zakresem obecnej dyrektywy. Przepisy te zachowano w proponowanym rozporządzeniu. Również ochrona urządzeń końcowych jest już przysługującym prawem. Wykorzystanie możliwości urządzeń końcowych użytkownika w zakresie przechowywania danych odbywa się w sposób neutralny pod względem technologicznym. Dlatego też nie tylko pliki cookie, ale wszystkie technologie śledzenia podlegają już zgodzie użytkownika lub jednemu z wyjątków określonych w dyrektywie o prywatności i łączności elektronicznej.

Ponadto proponowane rozporządzenie zmienione przez współprawodawców wprowadza kilka nowych wyjątków zaproponowanych przez Grupę Roboczą Art. 29[2], takich jak aktualizacje w zakresie bezpieczeństwa i pomiar odbiorców. Wyjątki te dotyczą konkretnych rodzajów przetwarzania, stanowiących bardzo ograniczone zagrożenie dla prywatności użytkowników.

[1] Zgodnie z definicją w WP216, przy czym dane poddane pseudonimizacji pozostają danymi osobowymi.

[2] Zob. opinie Grupy Roboczej WP194 oraz WP240.

3. Proponowane rozporządzenie ma na celu zapewnienie jego jednolitego stosowania we wszystkich państwach członkowskich oraz w odniesieniu do wszystkich rodzajów administratorów danych.

Obecna dyrektywa o prywatności i łączności elektronicznej nie ma zastosowania do usług łączności elektronicznej oferowanych przez dostawców działających w internecie, mimo że świadczą oni usługę równoważną pod względem funkcjonalnym.
Dostawcy ci będą jednak objęci zakresem proponowanego rozporządzenia. EROD podkreśla, że rozszerzenie zakresu stosowania rozporządzenia na usługi równoważne pod względem funkcjonalnym, w tym tzw. usług OTT, jest istotnym elementem reformy. Należy unikać wszelkich proponowanych zmian w projekcie rozporządzenia, które mogłyby podważyć ten cel (np. wszelkich propozycji zmierzających do ograniczenia zakresu ochrony do danych komunikacyjnych w trakcie przesyłu), aby zagwarantować wszystkim dostawcom równe warunki działania.
Proponowane rozporządzenie ma również zastosowanie niezwłocznie po zebraniu danych dotyczących zachowania użytkownika, bez względu na to, czy utworzył on konto w celu skorzystania z usługi. Takie podejście nie tylko zapewni użytkownikom usług ochronę, na jaką zasługują, ale także umożliwi uczciwą konkurencję między administratorami danych. Należy zauważyć, że zgoda, którą należy uzyskać na mocy rozporządzenia o e-prywatności, ma takie samo znaczenie jak zgoda na podstawie RODO. W szczególności wymóg dobrowolnego charakteru zgody uniemożliwi usługodawcom stosowanie tzw. *cookie walls*[3], a obowiązek uzyskania konkretnej zgody stworzy równe warunki działania dla usługodawców, niezależnie od tego, czy użytkownik był zalogowany.
Ponadto ustanowienie szczególnych sankcji za naruszenie rozporządzenia o e-prywatności, w połączeniu z rozszerzonym zakresem terytorialnym (oba te środki stanowią odzwierciedlenie przepisów RODO), zapewni organom ochrony danych skuteczne uprawnienia, które umożliwią im egzekwowanie stosowania rozporządzenia w odniesieniu do wszystkich narzędzi komunikacji elektronicznej wykorzystywanych przez użytkowników z UE.

4. Nowe rozporządzenie musi egzekwować wymóg uzyskania zgody używanie plików cookie i podobnych technologii oraz musi oferować dostawców usług narzędzia techniczne umożliwiające im uzyskanie tej zgody.

Zgodnie z wnioskiem Komisji Europejskiej art. 10 rozporządzenia ma zapewnić użytkownikom kontrolę nad wykorzystaniem możliwości ich urządzeń końcowych w zakresie przechowywania. Parlament zmodyfikował brzmienie art. 10 w celu wprowadzenia wymogu domyślnej ochrony prywatności w ustawieniach oprogramowania oraz dla zapewnienia rozwiązania technicznego służącego uzyskiwaniu ważnej zgody przez strony internetowe.
EROD w pełni popiera zaostrzenie tego artykułu i uważa, że powinien on wyraźnie odnosić się do systemów operacyjnych smartfonów, tabletów i wszelkich innych aplikacji klienckich, aby zagwarantować uwzględnianie w aplikacjach komunikacyjnych decyzji użytkowników niezależnie od środków technicznych.
Ponadto ustawienia ochrony prywatności powinny ułatwiać wyrażenie i wycofanie zgody w prosty, wiążący i możliwy do wyegzekwowania sposób wobec wszystkich stron, a użytkownicy powinni mieć możliwość dokonania przy instalacji jasnego wyboru, umożliwiającego im wyrażenie zgody, jeśli zechcą. Ponadto strony internetowe i aplikacje mobilne powinny mieć możliwość uzyskania zgody w sposób zgodny z RODO w ustawieniach prywatności.

5. Wnioski

EROD uważa, że:

- Rozporządzenie o e-prywatności nie powinno prowadzić do obniżenia poziomu ochrony zapewnianej obecnie przez dyrektywę o prywatności i łączności elektronicznej.
- Rozporządzenie o e-prywatności powinno zapewniać ochronę wszystkich rodzajów łączności elektronicznej, w tym w ramach usług OTT, w sposób neutralny pod względem technologicznym.
- Przed przetwarzaniem danych pochodzących z łączności elektronicznej lub wykorzystaniem możliwości urządzeń końcowych użytkownika w zakresie przechowywania lub przetwarzania należy systematycznie uzyskiwać zgodę użytkownika w sposób wykonalny technicznie i możliwy do wyegzekwowania. Nie należy wprowadzać wyjątków umożliwiających przetwarzanie danych w oparciu o „prawnie uzasadniony interes" administratora danych ani w ogólnym celu wykonania umowy.
- Art. 10 powinien przewidywać skuteczny sposób uzyskiwania zgody na stronach internetowych i w aplikacjach mobilnych. W ogólniejszym ujęciu ustawienia powinny domyślnie chronić prywatność użytkowników, a zapytanie użytkownika o wybór ustawienia powinno następować po przedstawieniu mu stosownych i przejrzystych informacji. W tym względzie rozporządzenie powinno pozostać neutralne pod względem technicznym, aby jego stosowanie było spójne niezależnie od konkretnych okoliczności.
- W przypadku wprowadzenia jakichkolwiek doraźnych wyjątków rozważanych przez prawodawców, oprócz tych już uwzględnionych w projektach Komisji i Parlamentu, należy stosować najwyższy stopień kontroli. Szczególnie rygorystycznej kontroli wymagają wszelkie szeroko ujmowane wyjątki dotyczące przypadków, w których „organ publiczny" zwraca się o przetwarzanie danych; projekt nie powinien zezwalać na masowe monitorowanie lokalizacji użytkowników ani na przetwarzanie ich metadanych.
- Aby zapewnić dobrowolność zgody, jak wymaga tego RODO, dostęp do usług i funkcji nie może być uzależniony od zgody użytkownika na przetwarzanie danych osobowych lub informacji przetwarzanych przez urządzenia końcowe użytkownika bądź związanych z takimi urządzeniami, co oznacza, że należy wyraźnie zabronić stosowania *cookie walls*.
- Należy zachęcać do stosowania danych pochodzących z łączności elektronicznej poddanych rzeczywistej anonimizacji.
- Wymienione zmiany zapewnią ochronę prywatności użytkowników końcowych we wszelkich odnośnych kontekstach oraz zapobiegną wszelkim zakłóceniom konkurencji.

[3] *Cookie wall* uniemożliwia dostęp do strony internetowej lub usługi użytkownikom, którzy nie wyrażają zgody na stosowanie plików cookie.



EDPB Document on

Terms of Reference of the EDPB Support Pool of Experts

Adopted on 15 December 2020

Table of contents

1 Terminology ... 3
2 Objectives ... 3
3 Scope ... 3
4 Support activities ... 5
5 Legal basis ... 5
5.1 Creation of the SPE ... 5
5.2 Deployment of the SPE ... 5
6 Key principles ... 7
6.1 Voluntary ... 7
6.2 Confidentiality and applicable law ... 7
6.3 Coordination ... 7
7 Composition of the SPE ... 8
7.1 EDPB experts ... 8
7.2 External experts ... 8
7.3 Reporting and evaluation ... 8
7.4 Budget and accountability ... 8
8 Financial support ... 9
8.1 EDPB experts ... 9
8.2 External experts ... 9

Adopted

1 TERMINOLOGY

1. For purposes of these Terms of Reference, the following terminology is used:

   - **Support Pool of Experts**: a pool of experts established in the context of the EDPB in order to assist in the carrying out of investigations and enforcement activities of significant common interest, comprising both EDPB experts and external experts.
   - **EDPB expert**: an expert employed by an EDPB member[1] or the EDPB Secretariat who is available to provide expertise relevant to an investigation or enforcement activity carried out by another supervisory authority.
   - **External expert**: an expert who is not employed by any member of the EDPB or EDPB Secretariat who is requested to provide expertise relevant to the investigation or enforcement activities of a supervisory authority against a fee, following the successful completion of the relevant selection process.

2 OBJECTIVES

2. The objective of the SPE is to contribute to a high and consistent level of protection of personal data throughout the EEA Member States by:

   (1) **Providing material support** to EDPB members in the form of expertise that is useful for investigations and enforcement activities of significant common interest and thereby promote better protection of data subjects; as well as

   (2) **Enhancing the cooperation** and solidarity between all EDPB members by sharing, reinforcing and complementing strengths and addressing operational needs.

3 SCOPE

3. The SPE will be deployed in order to support **investigations and enforcement activities of significant common interest** for the members of the Board.

4. Investigations and enforcement activities of significant common interest may for example concern cases involving major global companies whose activities have a substantial impact on the protection of personal data of individuals across the EEA.

5. While the need for additional support may be greatest in large and complex cases, the SPE may also be useful for smaller, yet strategically important matters. For example, there may be cases that are in first instance only of national importance, yet could set an important precedent for other EDPB Members as regards the interpretation of the GDPR.[2] The complexity of the subject matter or the fact that it will be likely to be resource-intensive will, however, remain an important consideration.

6. In other words, the possible deployment of the SPE is not limited to cases involving processing activities with EU-wide impact. Deployment in cases with primarily local (or regional) impact may also be envisaged, provided it relates to matters of significant common interest.

7. The SPE should not replace or pre-empt the ordinary discussions or exchanges that take place at the level of expert subgroups, where EDPB members can discuss both practical issues related to investigation and enforcement as well as matters of legal interpretation of the GDPR. For the SPE to be deployed there should also be an actual **operational need** (i.e. the supervisory authority in charge would have difficulty to proceed with its investigation or enforcement activity without receiving additional support going beyond the mere exchange of views or general discussion of the experiences from other supervisory authorities).[3]

8. **N.B.: Relationship to Coordinated Enforcement Framework (CEF)**:

   - The SPE has no direct relationship with the CEF.
   - Whereas the CEF provides a provides a structure for coordinating recurring annual activities by EDPB members ("topics for coordinated action"), the SPE provides a framework for sharing and combining resources.
   - Whereas the CEF identifies topics for coordinated action on an annual basis, deployment of the SPE is determined on an ad hoc (case-by-case) basis, in light of the operational needs of individual EDPB members in relation to a particular case.

   It is not excluded that the SPE is deployed to support the operational needs of one or more EDPB members in the context of a particular coordinated action, to be decided on a case-by-case basis.

[1] For purposes of these Terms of Reference, the term "EDPB member" should be understood as referring to all EEA national supervisory authorities (including the DE Länder SAs) as well as the EDPS.
[2] This may be particularly relevant in the absence of relevant guidelines or other common position of the EDPB on the matter.

[3] Chapter VII GDPR sets out various mechanisms for cooperation among supervisory authorities that include a.o. exchange of information, mutual assistance and joint operations. The precise purpose and nature of the support activity will be determinative in identifying the appropriate cooperation mechanism. See also Section 5.2 (Deployment of SPE).

4 SUPPORT ACTIVITIES

9. Supervisory authorities may require different types of expertise at different stages of their investigation and enforcement activities. As a result, there are **many different types of support** activities (types of expertise) that can be provided which include, without being limited to:

   - **analytical support** (e.g., sharing /explaining of a methodology for the carrying out of an inspection or calculating an administrative fine, legal analysis of a matter of EU law, a survey of the state of the art in a particular type of technology, …);
   - assisting in the **performance findings** of a forensic nature (e.g., in the context of an on-site or remote data protection audit);
   - assisting in the preparation of **investigative reports** on the basis of evidence collected.

10. The need for additional expertise is not always clear at the outset of an investigation or enforcement activity. Additional expertise may also be needed at later stages in the investigative and/or enforcement process (e.g. when preparing a fining decision; or in the context of an appeal).

11. The SPE may also have a more limited scope in terms of the types of support activities during the pilot phase (e.g. limited to the investigative phase).

5 LEGAL BASIS

5.1 Creation of the SPE

12. The legal basis for the creation of the SPE within the context of the EDPB can be found in Article 70 (1) (u) and (v) and Article 75 of the GDPR:

13. **Article 70(1)(u) GDPR** provides that the Board shall "*promote the cooperation and the effective bilateral and multilateral exchange of information and best practices between the supervisory authorities*".

14. **Article 70(1)(v) GDPR** provides that the Board shall "*promote common training programmes and facilitate personnel exchanges between the supervisory authorities and, where appropriate, with the supervisory authorities of third countries or with international organisations*".

15. **Article 75** of the GDPR provides that the Secretariat shall provide analytical, administrative and logistical support to the Board and shall be responsible for the communication between the members of the Board.

5.2 Deployment of the SPE

16. The legal basis for EDPB members to contribute to and receive assistance from the SPE can be found in Articles 57(1)(g) and (t) GDPR, Section 1 of Chapter VII of the GDPR (Articles 60-62) as well as Article 61 of Regulation (EU) 2018/1725 (EUDPR).

17. **Article 57(1)(g)** GDPR provides that each supervisory authority shall "*cooperate with, including sharing information and provide mutual assistance to, other supervisory authorities with a view to ensuring the consistency of application and enforcement of this Regulation*".[4]

18. **Article 57(1)(t)** GDPR provides that each supervisory authority shall contribute to the activities of the Board.

19. **Article 61(1)** GDPR provides that supervisory authorities "*shall provide each other with relevant information and mutual assistance in order to implement and apply this Regulation in a consistent manner, and shall put in place measures for effective cooperation with one another. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out prior authorisations and consultations, inspections and investigations.*"

20. **Article 62(1)** GDPR provides that supervisory authorities "*shall, where appropriate, conduct joint operations including joint investigations and joint enforcement measures in which members or staff of the supervisory authorities of other Member States are involved.*"

21. Experts can only support investigations and enforcement activities **in accordance with the GDPR and other applicable legislation**. Much like the CEF, the SPE supports and builds on mechanisms for cooperation that are in the GDPR. This means that the SPE is without prejudice to the functioning of the cooperation- and consistency mechanisms under the GDPR and the other tasks and the powers of the EDPB and EDPB members.[5] There is also **no obligation** whatsoever for EDPB members to submit a request or offer of support via the SPE prior to initiating any of the cooperation mechanisms provided by GDPR. In other words: the creation of the SPE in no way precludes SAs from extending support to one another in any case they consider appropriate.[6]

22. Chapter VII GDPR sets out various mechanisms for cooperation among supervisory authorities that include a.o. exchange of information, mutual assistance and joint operations. The precise purpose and nature of the support activity will be determinative in identifying the appropriate cooperation mechanism. In practice, the involvement of EDPB experts may take the form of a sharing of information (Article 57(1)g, mutual assistance (voluntary/formal[7]) (Article 61), or joint operation (Article 62)[8]. As a

[4] Article 61 Regulation (EU) 2018/1725 (EUDPR) provides that *"[t]he European Data Protection Supervisor shall cooperate with national supervisory authorities and with the joint supervisory authority established under Article 25 of Council Decision 2009/917/JHA to the extent necessary for the performance of their respective duties, in particular by providing each other with relevant information, asking each other to exercise their powers and responding to each other's requests."* See also Art. 26 of the EDPS Rules of Procedure (*"Article 26 Cooperation with national supervisory authorities under Article 61 of the Regulation)*.

[5] Any involvement of the SPE must therefore be mindful of the division of competences between EDPB and national SAs, making the most of the tasks and competences allocated to both. In the same vein, the establishment of the SPE shall be without prejudice to any other existing provisions or arrangements on cooperation or the setting up or operation of joint operations.

[6] The SPE primarily seeks to *facilitate* the matching of available expertise with operational needs. It does not in any way prevent EDPB members and national supervisory authorities from directly providing each other with support whenever the operational need arises in accordance with cooperation mechanisms of the GDPR.

[7] The ability to seek (and the obligation to give) mutual assistance applies to any case in which an SA requires the assistance of another SA for the performance of its tasks. Article 61 GDPR does not have to concern cross-border processing in order to be triggered. Article 61 GDPR can be used, for example, as a tool to share findings between the SAs involved.

[8] Article 62 GDPR provides rules for joint operations by the supervisory authorities, including joint investigations and joint enforcement measures. The application of Article 62 GDPR is not limited to cross-border cases. In case of a joint operation within the meaning of Article 62 GDPR, any investigative powers conferred upon an EDPB expert may only be exercised with the approval, under the guidance and in the presence of members or staff of

result, the appropriate cooperation mechanism (i.e. the legal basis for a particular form of cooperation) will need to be determined on a case-by-case basis prior to deployment, taking into account also any limitations imposed by national law.

6 KEY PRINCIPLES

6.1 Voluntary

23. The involvement of EDPB experts or external experts requires the agreement of the EDPB member responsible for the investigation and/or enforcement activity. In case of EDPB experts, it also requires the agreement of their employer.

24. Any EDPB member may request or propose the involvement of one or more experts from the SPE to support an investigation and/or enforcement activity.

25. Experts will provide their expertise in accordance with the purpose, nature and duration of the support activity agreed by the EDPB member responsible for the investigation and/or enforcement activity.

26. Each EDPB member remains responsible for investigations and follow-up enforcement action in their respective jurisdictions.

6.2 Confidentiality and applicable law

27. Experts will be required to support investigations and enforcement activities in compliance with the legislation applicable to the EDPB member responsible for the investigation and/or enforcement activities.

28. Experts will be required to respect at least equivalent rules of confidentiality as the staff of the EDPB member responsible for the investigation or enforcement activities, which may require the signing of a non-disclosure agreement and to provide further guarantees of impartiality.

6.3 Coordination

29. The SEC will be charged with ensuring coordination of the SPE, in accordance with Articles 70(1)(u)-(v) and 75(5)-(6) GDPR.

30. The SEC will liaise with the contact points of the SPE in order to help fill requests for support (i.e. to match experts with the operational needs articulated in the requests).

7 COMPOSITION OF THE SPE

7.1 EDPB experts

31. An EDPB expert is an expert employed by an EDPB member or the EDPB Secretariat who is available to provide expertise relevant to an investigation or enforcement activity carried out by an(other) EDPB member.

32. EDPB experts continue to be employed by their respective employer but provide assistance to an(other) EDPB member for the purposes, activities and duration agreed between their employer and the EDPB member responsible for the investigations and/or enforcement activity.

7.2 External experts

33. An external expert is a person who is not employed by any member of the EDPB or the EDPB Secretariat, yet has demonstrated expertise that is relevant to the needs of an investigation or enforcement activity.

34. External experts provide their services against the payment of a fee.[9] External experts are admitted to the Support Pool of Experts following a call for expressions of interest and the successful completion of the selection process. The list drawn up on the basis of the call for expression of interest does not imply any obligation on the part of the EDPB to award a service contract (by the use of an order form) to the successful applicants.

35. The involvement of external experts may be necessary to ensure that highly specialised knowledge (e.g., in relation to forensics) can be made available to complement the expertise present in the supervisory authorities in order to address the operational needs of a specific case. As a result, external experts should only be selected on a subordinated basis , i.e. after it has been determined that no EDPB expert is available to provide the necessary support for the requesting EDPB member within the requested timeframe due to reasons of capacity.

7.3 Reporting and evaluation

36. The SEC will provide regular reports (minimum twice a year). For example, in case the number of requests risks to exceed available resources, the Plenary may be informed to help determine priorities, taking into account also the resources that remain for the relevant period.

37. The SEC will also make an annual evaluation report of the SPE initiative.

7.4 Budget and accountability

38. The funding of eligible expenses of the SPE will be part of the EDPB budget[10].

---

the host supervisory authority and insofar the law of the Member State of the host authority permits. The EDPB expert shall be subject to the Member State law of the host supervisory authority. The scope of application of Article 62 is limited to supervisory authorities. As a result, only experts employed by EDPB members can participate in Article 62 joint operations. Experts employed by the EDPB Secretariat cannot participate in Article 62 Joint Operations in the same manner as EDPB members.

[9] Without prejudice to particular specifications agreed for a specific assignment, which will be enclosed with the request sent to the expert selected, the volumes, deadlines and remuneration for the various forms of expertise are set out in a table included with the call for expressions of interest, as well as the maximum total amount that can be paid to each individual expert.

[10] The EDPB Secretariat will plan for the inclusion of additional budget for SPE in the preparation of 2022 Budget that will be carried out beginning of 2021.

8 FINANCIAL SUPPORT

8.1 EDPB experts

39. The salary of EDPB experts remains covered by their employer, as they remain part of the staff of their employer. Each EDPB Member as well as the EDPB SEC will therefore need to consider this in their respective budget plans.

40. Upon confirmation of eligibility, the EDPB may, subject to budget availability, assist by reimbursing the costs of two common areas of expenditure:

    (1) travel and, subject to further assessment, accommodation and/or daily allowances (in case physical presence is required),

    (2) translation (e.g., of investigative reports) in specific cases.

8.2 External experts

41. Upon confirmation of eligibility, the EDPB may assist by reimbursing the costs relating to travel and daily allowance (in case physical presence is required).

42. Fees of external experts may also be eligible for reimbursement, subject to budgetary availability and approval of the EU Budgetary Authority as regards allocation of EDPB Budget and provisioning of the necessary financial resources. Contact may also be made with the European Commission in case the SPE could also rely EU funding programmes (e.g., in the form of a project grant).

Adopted



EDPB Document on

Coordinated Enforcement Framework

under Regulation 2016/679

Adopted on 20 October 2020

EXECUTIVE SUMMARY

Definition

The Coordinated Enforcement Framework (CEF) provides a structure for coordinating recurring annual activities by EDPB Supervisory Authorities (throughout this document, this is called an 'annual coordinated action'). The annual coordinated action focuses on a pre-defined topic and allows SAs to pursue this topic using the agreed-upon methodology. The CEF itself provides the procedural outline within which the coordinated action can take place (the 'rulebook').

Objectives

The objective of the CEF is to facilitate joint actions in a flexible but coordinated manner, ranging from joint awareness raising and information gathering to enforcement sweeps and joint investigations. The purpose of recurring annual coordinated actions is to promote compliance, to empower data subjects to exercise their rights, to raise awareness, and/or to increase the knowledge of SAs.

Legal Basis

According to Article 61(1) GDPR, SAs shall put in place measures for effective cooperation with one another. Article 57(1)(g) GDPR tasks SAs with cooperating, including sharing information and providing mutual assistance to other SAs with a view to ensuring the consistency of application and enforcement of the GDPR.

The Relationship between the CEF and Chapter VII GDPR

The one-stop-shop mechanism remains unaffected by the CEF and applies whenever cross-border processing activities are concerned. Mutual assistance (Article 61 GDPR) can be used as a tool within the annual coordinated action, but should be limited to its voluntary form where possible. Lastly, it is possible to use joint operations (Article 62 GDPR) as a methodology to perform an annual coordinated action, but other, less formal methodologies are possible as well.

Timeframe

The coordinated action will, in principle and if the resources allow, cover a period of one year. If the CEF is adopted in the second quarter of 2020, the focus for the first coordinated action will be identified in the last two quarters of 2020, the coordinated action will be executed in the first and second quarters of 2021 and in the third quarter of 2021, the final report will be drafted and a new coordinated action will be prepared.

Table of contents

Executive Summary 2

1 **Introduction** 5

2 **What is the Coordinated Enforcement Framework?** 5

2.1 Summary of the CEF life-cycle 5

2.2 Legal basis and division of competences 7

2.3 Relationship with the cooperation mechanisms under the GDPR 7

2.3.1 One-stop-shop mechanism 7

2.3.2 Mutual assistance 8

2.3.3 Joint operations 8

The European Data Protection Board

Having regard to Article 70(1)(u) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter "GDPR"),

Having regard to Article 61 (1) and Article 57 (1)(g) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, (hereinafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,

Having regard to its Rules of Procedure,

HAS ADOPTED THE FOLLOWING DOCUMENT

1 INTRODUCTION

1. The European Data Protection Board (EDPB) is an independent European body, which is tasked to ensure the consistent application of data protection rules throughout the European Union (EU), and promotes cooperation between the EU's data protection authorities. The EDPB is composed of the heads of the Supervisory Authorities (SA) and the European Data Protection Supervisor (EDPS) or their representatives.

2. All SAs are tasked with the supervision and enforcement of the General Data Protection Regulation (GDPR), which applies from 25 May 2018. The GDPR safeguards the fundamental right to protection of personal data and facilitates free movement of personal data (Article 1 GDPR). To that end, the GDPR contains a catalogue of rights for data subjects and imposes obligations upon controllers and processors – not just with regard to respecting the rights of data subjects, but also concerning technical and organizational measures associated with security aspects. The GDPR gives the SAs a fundamental role in supervision of compliance with these provisions, as well as a duty of cooperation between the authorities and coherence in their decisions that contribute to the free circulation of data among the Member States, resulting in a harmonized European space in terms of data protection.

3. The EDPB supports coherence in approach through consistency procedures, regular meetings and (internal) guidance. In addition, the GDPR emphasizes cooperation between national SAs and introduces a one-stop-shop mechanism for case handling. The Coordinated Enforcement Framework (CEF) that is introduced in this document supports and builds on mechanisms for cooperation that are in the GDPR. Different from reactive action (e.g. complaint handling), action under the CEF is intended to be proactive.

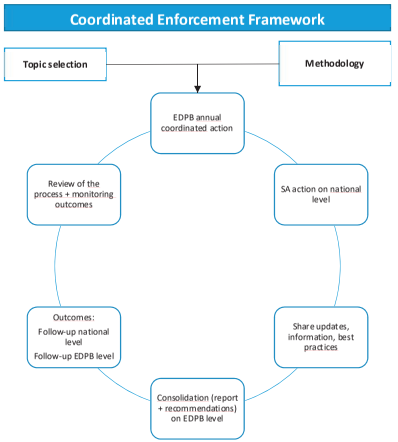
2 WHAT IS THE COORDINATED ENFORCEMENT FRAMEWORK?

4. The Coordinated Enforcement Framework (CEF) provides a **structure for coordinating recurring annual activities** by EDPB Supervisory Authorities (throughout this document, this is called an 'annual coordinated action'). The annual coordinated action focuses on a pre-defined topic which participating SAs may pursue using a pre-defined methodology.

5. The CEF is the foundation on which the annual coordinated action is built (the 'rulebook' for coordinated action). The objective of the CEF is to facilitate joint actions in the broad sense in a flexible but coordinated manner, ranging from joint awareness raising and information gathering to an enforcement sweep and joint investigations. This ultimately contributes to compliance with the GDPR; ensuring the rights and freedoms of citizens and reducing the risk of services based on new technologies in the field of data protection.

2.1 Summary of the CEF life-cycle

6. The CEF life-cycle, including the annual coordinated action, can be visualised as follows:



7. As this schematic overview illustrates, the Coordinated Enforcement Framework is the structure in which an annual coordinated action can take place. In principle, each year, the EDPB decides upon a topic for coordinated action and agrees on the methodology that goes along with it. After that, the national SAs determine the scope of their national execution of the annual coordinated action and carry it out over the course of – approximately – one year. Participation in the coordinated action for any given year is not mandatory, though decisions regarding topic selection and methodology should be as inclusive as possible with an aim to maximize SA participation in any agreed annual coordinated action.

8. For the duration of the chosen annual coordinated action, national SAs will share updates on the progress, relevant information and – where applicable – best practices. All national findings will be consolidated in a report on EDPB-level, in which the participating SAs will make recommendations as to the follow-up of the annual action (for instance follow-up enforcement action on a national level, or guidance on an EDPB-level). After the coordinated action has taken place and recommendations have been made, the participating SAs will review the process as a whole, in order to fine-tune the CEF and simplify coordinated actions for the coming years. Where follow-up action is recommended, the implementation of such action will be monitored.

2.2 Legal basis and division of competences

9. The GDPR is the basis and the authority under which the annual coordinated action within the Coordinated Enforcement Framework will be executed. This means that other relevant EU legislation (such as Directive 2016/680) will be left outside the scope. The GDPR both determines the scope of the action ('what type of non-compliance do we address to best safeguard the rights of data subjects') as well as the legal basis on which action can be taken. In that sense, it almost goes without saying that the field of application of any action by the EDPB and national SAs should fall within the material and territorial scope of the GDPR. To that end, the CEF and the annual coordinated action are confined by the limits of Article 2 (material scope) and Article 3 (territorial scope) of the GDPR.

10. The legal basis for the CEF is found in Article 57(1)(g), which gives national SAs the competence to cooperate "with, including sharing information and provide mutual assistance to, other supervisory authorities with a view to ensuring the consistency of application and enforcement of this Regulation." National SAs participating in the annual coordinated action do so on the basis of their advisory powers and monitoring- and awareness-raising tasks outlined in Articles 57(1) and 58(3) GDPR. Additionally, if SAs decide to use investigative powers or impose measures, they may do so on the basis of Articles 58(1) and (2) GDPR.

11. Turning to the division of competences between the EDPB and the national SAs, the CEF assumes as a starting point that investigation and enforcement of the GDPR primarily rests with the national SAs (cf. Article 58 GDPR), whereas the EDPB is tasked with ensuring the consistent application of the GDPR (cf. Article 70 GDPR). To that end, only national SAs are responsible for investigations and follow-up enforcement action in their respective jurisdictions. The EDPB, in turn, provides the platform to share and combine national efforts and takes responsibility where the outcomes of the annual coordinated action call for guidance or recommendations in the fields covered by Article 70(1) GDPR.

2.3 Relationship with the cooperation mechanisms under the GDPR

12. The CEF and the annual coordinated action are without prejudice to the functioning of the cooperation- and consistency mechanisms under the GDPR and the other tasks and the powers of the EDPB and the national SAs. Any coordinated enforcement action should be mindful of the division of competences between EDPB and national SAs, making the most of the tasks and competences allocated to both.

2.3.1 One-stop-shop mechanism

13. The OSS regulates the cooperation of the responsible supervisory authorities for cross-border data processing within the EU. The OSS has a dual objective: (i) to give the responsible bodies and processors the possibility of turning to a supervisory authority as the central point of contact for the whole of the European Union and (ii) to give concerned persons a local body with the necessary powers and competences to help them enforce their data protection rights. If a certain processing is considered cross-border processing in the sense of Article 4(23) GDPR, the application of the OSS is mandatory – even if this cross-border processing is found in the context of an annual coordinated action. If this happens, the procedures outlined for dealing with cross border cases should be followed and the best course of action should be determined on a case by case basis.

14. Since the annual coordinated action should not lead to an unreasonable burden upon a small number of LSAs and because all participating SAs should have the competence to examine the controllers/processors involved, it should not be the intention from the offset to trigger the OSS during an annual coordinated action. However, depending on the scope of the coordinated action, it is possible that the OSS becomes applicable nonetheless, for instance if it is discovered that a controller/processor under examination engages in cross-border processing relevant to the topic. If this happens, the procedures outlined for dealing with cross-border cases should be followed and the best course of action should be determined on a case-by-case basis. It should be borne in mind that in these cases, Articles 61 and 62 GDPR can be used as tools to alleviate unnecessary burden upon the (newly found) LSA.

2.3.2 Mutual assistance

15. The obligation to give mutual assistance applies to any case in which an SA requires the assistance of another SA for the performance of its tasks. Essentially, Article 61 GDPR regulates the obligations of the requested SA and the consequences of breach of those obligations. Article 61 GDPR does not have to concern cross-border processing in order to be triggered.

16. Article 61 GDPR and the CEF are two distinct instruments. The first allows for SAs to request each other's assistance regarding specific issues/cases. The latter facilitates that multiple SAs look into the same issue in their respective countries at the same time, and provides a framework under which they can discuss their findings and intended next steps. However, Article 61 GDPR can be used as a tool within the CEF to share findings or ask information between the participating SAs – especially the *voluntary* mutual assistance that is available on the IMI system. Triggering a formal mutual assistance procedure should be avoided in the course of the CEF due to the voluntary nature of participation and should – in accordance with the Article 61 Process Guide – be reserved for cases in which an informal request is impossible.

2.3.3 Joint operations

17. Article 62 GDPR provides rules for joint operations by the supervisory authorities, including joint investigations and joint enforcement measures. A joint operation occurs where two or more SAs join forces in order to act toward a commonly agreed purpose. In order to do so, SAs make available their resources including their skills and staff. The application of Article 62 GDPR is not limited to crossborder cases.

18. In order to distinguish the CEF from an Article 62 joint operation, it is important to bear in mind that the CEF is a broader framework that allows SAs to use various methodologies to look into a predefined issue on their respective national levels. Examples of such methodologies are conducting a joint survey, conducting a sweep or engaging in joint awareness raising. Conducting a joint operation in the sense of Article 62 GDPR is also one of the methodologies that can be used. Therefore, the CEF is the overarching framework in which Article 62 GDPR can be used as a tool for an annual coordinated action. For that reason, joint operations are not further elaborated upon in this document.

For the European Data Protection Board

The Chair
(Andrea Jelinek)



First overview on the implementation of the GDPR and the roles and means of the national supervisory authorities

Executive Summary

This document sets out an overview of the implementation and enforcement of the General Data Protection Regulation (GDPR) covering both the cooperation mechanism and the consistency findings.

In comparison with the EC Directive 95/46/EC, where Supervisory Authorities (SAs) were working separately even on cross-border cases, the GDPR created a duty for the SAs to cooperate in order to provide a consistent application of the GDPR. In addition to that, the European Data Protection Board (EDPB) provides a consistency mechanism to further foster the harmonisation.

Nine months after the entry into application of the GDPR, the members of the EDPB are of the opinion that the GDPR cooperation and consistency mechanism work quite well in practice. The national supervisory authorities make daily efforts to facilitate this cooperation, which implies numerous exchanges (written and oral) between them.

These cooperation duties lead to extra workloads, additional time dealing with cases and have an impact on the budget of the regulators. The handling of cross border cases takes time, due to the cooperation, to the need to carry out thorough investigations and in order to national procedural rules. The national SAs have to tackle these challenges regarding the harmonized protection and enforcement of the GDPR.

Until now, there are 6 final One-Stop-Shop cases.

The experiences of the EDPB regarding consistency is – up to now – limited, as no dispute resolution through this new EU body was necessary during the reported period.

I. Cooperation mechanism among SAs and the consistency mechanism of the EDPB

Cooperation mechanism

The GDPR requires close cooperation between SAs of EEA (EU-28 + Iceland, Norway and Liechtenstein) in cases implying a cross-border component and supports this by using the following tools:

- the mutual assistance,
- the joint operation,
- the One-Stop-Shop cooperation mechanism, which introduces the obligatory intervention of a Lead Supervisory Authority for the cross-border cases.

The cooperation on cross-border cases (ie. on the basis of complaints from individuals) is conducted by the national supervisory authorities. The EDPB does not deal with those cases unless a dispute arises between the authorities or in the case of urgency.

Consistency mechanism

One of the main tasks of the EDPB is to ensure the consistent application of the GDPR.

One opportunity to ensure consistency is to provide **general guidance** on the interpretation of the GDPR, which will contribute to a common understanding and application of the provisions by the stakeholders, the supervisory authorities and the public in general. Since 25 May 2018, the EDPB has endorsed 16 guidelines prepared by the Article 29 Working Party (predecessor of the EDPB) and has adopted 5 additional guidelines.

Another opportunity is to adopt **consistency opinions and decisions**. These decisions mainly address the national supervisory authorities and ensures a consistent application and enforcement of the GDPR.

Standardised communication:

To support the cooperation and the consistency mechanism among the EDPB members the DG Grow of the EU Commission, together with the EDPB Secretariat and the EDPB members, have customised an already existing IT system – the Internal Market Information system (IMI). This system was operational on the first day of the entry into application of the GDPR. This system provides a structured and confidential way to share information among the SAs.

The feedback of the national regulators on this system is really positive. A dedicated expert subgroup has been created to ensure the continuous enhancement of the system on the basis of the feedback collected via a dedicated IT Helpdesk support provided to the EDPB members by the EDPB Secretariat.

Before a case is produced in the case register of the system, the competent authorities have to be identified. This registry is the central database from which different procedures can be started, such as the mutual assistance, joint operation and One-Stop-Shop mechanism.

The scheme in the appendix provides an overview of the functioning of the system.

1. Cooperation Mechanism

a. Preliminary procedure to identify the lead and concerned supervisory authorities

Before starting a One-Stop-Shop procedure for cross-border cases, it is necessary to identify the authority that will lead the cooperation (Lead SA), and the other Concerned supervisory authorities (Concerned SA). The Lead SA will have to lead the cooperation procedure, draft the decision and the Concerned SAs will have the opportunity to raise objections.

The Lead SA is the authority within the EEA where the organisation subject to the investigation has its main establishment**.** The main establishment is identified as the central administration of the investigated company/organisation in the EU.

The EDPB created workflows in the IMI system to enable the SAs to identify their respective roles. The main purpose of this procedure is to define the roles at an early stage and to avoid objections on the question of competences at a later stage of the procedure.

In case of conflicting views regarding which authority should act as Lead SA**,** EDPB has the role of a dispute resolution body and issues a binding decision.

Since 25 May 2018, **642 procedures have been initiated to identify the Lead SA and the Concerned SAs** in cross-border cases. Out of the 642 procedures, **306 are closed and the Lead SA identified.**

Up to now, no dispute arose on the selection of the Lead SA.

24 EEA countries already initiated procedures and 26 SAs were proposed to act as lead SA.

b. Data base regarding cases with cross-border component

These cases will be registered in a central database from which different procedures can be initiated, such as the mutual assistance, joint operation and One-Stop-Shop mechanism.

Since 25 May 2018, 30 different EEA SAs have registered a total amount of **281 cases with cross-border component** in the IMI system.

The large part of the opened cases derived from **complaints by individuals (194 cases).** The rest of the cases (87) has other origins.

The **three main topics** of the cases are related to the **exercise of the data subjects' rights, to the consumer rights and to data breaches**.

c. One-Stop-Shop Mechanism

The GDPR provides a specific cooperation procedure (One-Stop-Shop) for cross-border cases. A cross border case emerges where the controller or the processor has an establishment in more than one Member State or where the data processing activity substantially affects individuals in more than one Member State.

The One-Stop-Shop mechanism implies a cooperation between the Lead SA and the Concerned SA. The Lead SA will lead the cooperation procedure and plays a key role in the process to reach consensus between the Concerned SAs and to reach a coordinated decision with regard to a data controller or processor.

The Lead SA first has to investigate the case while observing its national procedural rules (eg. provide the right to be heard to the affected persons). During this investigation phase, it can gather information from another supervisory authority via mutual assistance or conduct joint investigation, where foreseen in the respective national law.

The IMI system also offers the opportunity for the Lead SA to launch – if necessary - an **informal communication with all the Concerned SAs** to collect information to prepare its draft decision.

Once the Lead SA has completed the investigation, **it prepares a draft decision and communicates it** to the Concerned SAs. These can object to the draft decision, which either leads to a revised draft decision or triggers the dispute resolving mechanism of the board.

If a dispute arose on the draft decision and no consensus is found, the consistency mechanism is triggered and the case is referred to the EDPB. The EDPB will then act as a dispute resolution body and issue a binding decision on the case. The Lead SA will have to adopt its **final decision** on the basis of the decision of the EDPB.

If the Concerned SAs do not object to the initial draft decision, or the revised one, they are deemed in agreement with the draft decision. So, the Lead SA can adopt **its final decision.**

The IMI system offers different procedures to handle the One-Stop-Shop cases:

1. Informal consultation procedures,
2. Draft decisions or revised decision submitted by the Lead SA to the Concerned SAs,
3. Final One-Stop-Shop decisions submitted to the Concerned SAs and to the EDPB.

Since 25 May 2018, **45 One-Stop-Shop procedures** were **initiated by SAs from 14 different EEA countries**. The 45 procedures are at different stages: **23 are at the informal consultation level**, **16 are at draft decision** level and **6 are final decisions**.

These first final One-Stop-Shop decisions relate to the exercise of the rights of individuals (such as the right to erasure), the appropriate legal basis for data processing and data breach notifications.

The limited number of **One-Stop-Shop procedures can be explained because** the circulation of the **draft decision is the result of the investigation**s conducted by the Lead SA respecting national administrative procedural laws. The number of One-Stop-Shop procedures are **increasing steadily.**

d. Mutual assistance

The mutual assistance procedure allows each SAs to ask for information to other SAs but also to request any other measures for effective cooperation (such as prior authorisations, investigations, etc.).

The mutual assistance can be used for cross-border cases subject to the One-Stop-Shop procedure (as part of the preliminary phase to gather elements necessary before drafting a decision), or can also be used for national cases with cross-border component.

The IMI system enables the use of **informal mutual assistance**, **without any legal deadline** or the use of **formal mutual assistance** where the requested SA has **a legal deadline of 1 month** to reply to the request.

Since 25 May 2018, **444 mutual assistance requests (formal and informal)** have been triggered by **SAs from 18 different EEA countries**.

In 353 cases out of the 444 mutual assistance requests, **the answers were sent within 23 days**. The remaining 91 cases are ongoing, not yet answered by the requested SA.

e. Joint operations

The GDPR allows the SAs of different member states to carry out joint investigations and joint enforcement measures. The joint operations can be used in the context of cross-border cases subject to the One-Stop-Shop procedure (as part of the preliminary phase to gather elements necessary before the drafting a decision), or can also be used for national cases including a cross-border component.

Since 25 May 2018 to 31 January 2019, **no joint operations have been initiated**.

f. Assessment of the cooperation mechanism and suggestions for improvement by the SAs

In comparison with the EC Directive 95/46/EC where SAs were working separately even on cross border cases, the GDPR foresees a duty for the SAs to cooperate in order to provide a consistent application of the GDPR.

The national regulators adapted to this new situation. One of the advantages of the GDPR is to let some margin of manoeuvre for the SA to address those challenges.

However, the GDPR has been in application only for 9 months and there is still work to be done at the EDPB level to further streamline the procedure to make the system even more efficient. The question of the resources allocated to the authorities (and the possibility to recruit staff speaking also English) has impacts on the global efficiency of the system.

2. Consistency Mechanism

a. Consistency opinion

For some type of decisions, the national SAs have to require an opinion of the EDPB before being entitled to adopt its decision. This applies for instance to the approval of cross-border codes of conducts, the adoption of standardised contractual clauses, or the adoption of national lists describing the type of processing that must be subject to a Data Protection Impact Assessment.

The purpose of the consistency opinion issued by the EDPB is to guarantee the consistent application of the GDPR in cases where a competent SA wants to adopt those specific measures.

Each national SA, the Chair of the EDPB or the Commission can ask the EDPB to issue a consistency opinion on any matter of general application or producing effects in more than one Member State.

Since 25 May 2018, 28 opinions on the national lists of processing subject to a Data Protection Impact Assessment and 1 opinion on a draft administrative arrangement for the transfer of personal data between financial supervisory authorities (in the EEA and outside of the EEA) have been adopted by the EDPB. Currently there are 3 ongoing procedures which are related to binding corporate rules, to a draft standard contract between Controllers and Processors and to the interplay between the GDPR and the ePrivacy Directive, in particular as regards the competence of the national data protection supervisory authorities.

b. Dispute resolution

The EDPB intervenes as dispute resolution body and adopt binding decisions, in order to ensure the consistent application of the GDPR, in following cases:

- A dispute takes place within the One-Stop-Shop mechanism (a Concerned SA raises a relevant and reasoned objection which is not followed by the Lead SA);
- A disagreement takes place on the determination of the Lead SA;
- A SA does not request or does not follow a consistency opinion of the EDPB.

From 25 May 2018 to 18 February 2019, **no dispute resolutions were initiated**. This means that up to now, the SAs were able to reach consensus in all current cases, which is a good sign in terms of cooperation.

c. Assessment of the consistency mechanism and suggestion for improvement by the SAs

The following analysis reflects the views and impressions of the authorities in the context of this report.

Up to now, the EDPB did not have to act as a dispute resolution body, also due to the fact that the number of decisions resulting from the One-Stop-Shop cases is still relatively small.

Since the EDPB has so far focused mainly on the preparation of consistency opinions on national DPIA lists (on the national lists of processing subject to a Data Protection Impact Assessment) most authorities emphasised that the experience of the EDPB with the consistency mechanism in other areas is still limited. However, it is planned that in the coming months other types of national measures, such as BCRs, codes of conducts, standard contracts and issues related to certification will be submitted to the EDPB and thus trigger the consistency mechanism in other fields.

It was indicated that, already on the basis of the first experiences the consistency mechanisms was found to require many resources, to be time-consuming and to require the authorities to act swiftly within the given timeframe. In this context, a possible need to extend the deadlines was addressed.

II. Means and powers of the national supervisory authorities

1. Budget and human resources

Under the new legal framework, SAs wear two hats. They not only deal with their enhanced enforcement powers but are required to become more engaged, which implies the need for more budget and staff.

a. Budget

While, based on information provided by SAs from 26 EEA countries and the EDPS, in most cases an increase in the budget for 2018 and 2019 was observed, in two cases a decrease and in 3 cases no changes in the budget were noticed. According to information provided by the respective SAs, the latter phenomena can be explained by biannual plans for this period of time.

Although the majority of the 17 replying SAs stated that they would need an increase in the budget of 30-50%, almost none of them received the requested amount. There are some extreme examples where this need is close to or even 100 %.

b. Human resources

Based on information provided by SAs from 26 EEA countries and the EDPS, the majority of SAs have experienced an increase in the number of staff, while for 8 SAs the human resources did not change. For one SA, there was even a decrease in personnel.

Given the different scope of competences of the SAs (GDPR, e-Privacy, Freedom of Information), the requirements for more personnel also vary.

2. Implementation and enforcement of the GDPR at national level

The total number of cases reported by SAs from 31 EEA countries is 206.326. Three different types of the cases can be distinguished, namely cases based on complaints, cases based on data breach notifications and other types of cases. The majority of the cases are related to complaints, notably 94.622 while 64.684 were initiated on the basis of data breach notification by the controller.

52 % of these cases have already been closed and 1 % of these cases challenged before national court.

Corrective powers:

Regarding the corrective powers, the SAs have different measures to use:

- to issue warnings to a controller or processor that intended processing operations are likely to infringe the GDPR,
- to issue reprimands to a controller or a processor where processing operations have infringed the GDPR,
- to order the controller or the processor to comply with the data subject's requests or to bring processing operations into compliance with the GDPR,
- to impose administrative limitations, bans and fines.

SAs from 11 EEA countries have already imposed administrative fines according to Article 58.2 (i) GDPR. The total amount of the imposed fine is 55.955.871 EUR.

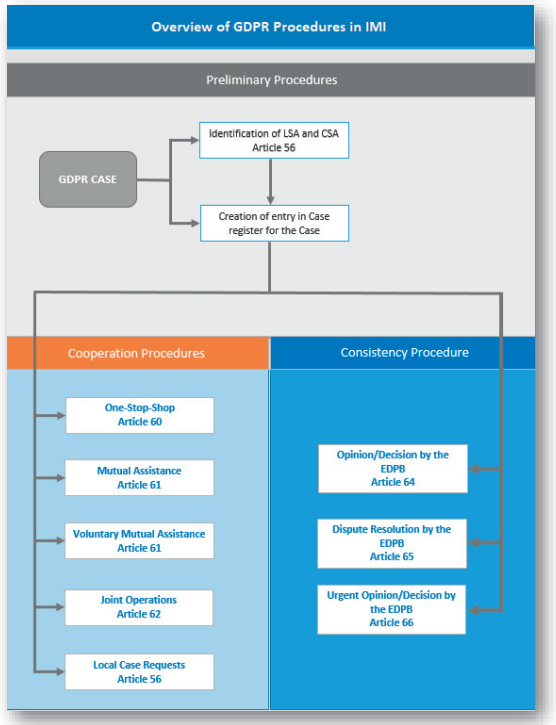
III. Conclusion

Nine months after the entry into application of the GDPR, the members of the EDPB are of the opinion that the GDPR works quite well in practice making use of the new way of cooperation including numerous daily exchanges. The One-Stop-Shop cases that have already led to an outcome tested some of the core principles of the GDPR and were resolved smoothly. So far, not a single cross-border case has been escalated to the EDPB level.

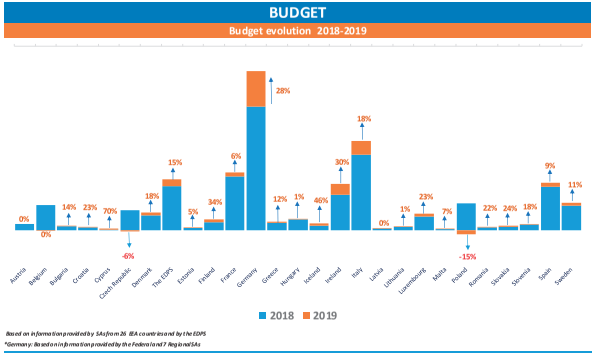
Despite the increase in the number of cases in the last months, the SAs reported that the workload is manageable for the moment, in large part thanks to a thorough preparation during the past two years by SAs, the Article 29 Working Party and by the Board.

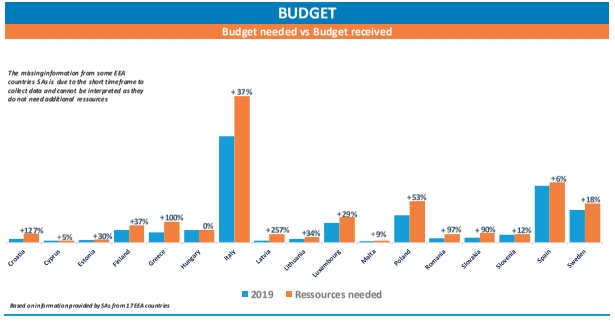
Appendix

Cooperation mechanism among SAs and the consistency mechanism of the EDPB

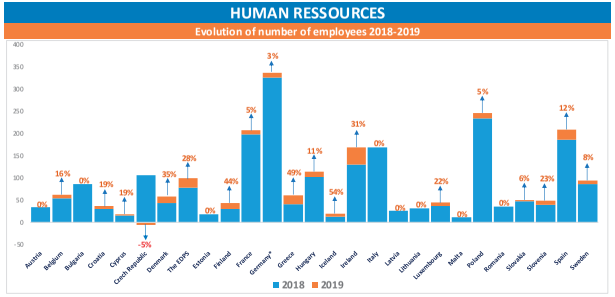


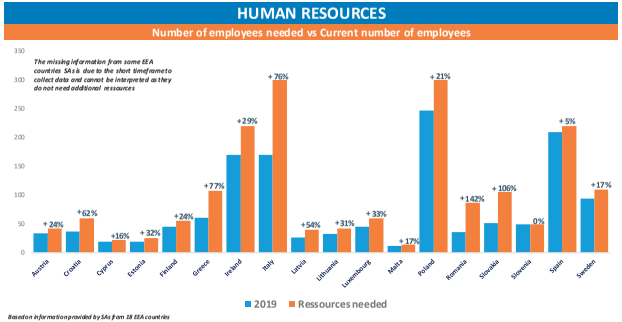
Budget





Human resources

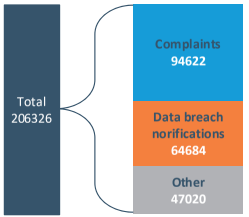




Implementation and enforcement of the GDPR at national level

NATIONAL CASES

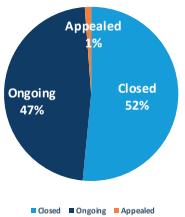
Number of cases per type



Based on information provided by SAs from 31 EEA countries
**Germany: Based on information provided by The Federal and 13 Regional SAs*

NATIONAL CASES

Number of cases per status



Based on information provided by SAs from 23 EEA countries (Case status information provided for 72818 cases)
**Germany: Based on information provided by The Federal and 5 Regional SAs*

FINES

Number of imposed fines



SAs from 11 EEA countries imposed a total of €55,955,871 fine

Based on information provided by SAs from 11 EEA countries
Germany: Based on information provided by 4 regional SAs



EDPB contribution to the consultation on a draft second additional protocol to the Council of Europe Convention on Cybercrime (Budapest Convention)

Brussels, 13th November 2019

Preliminary remarks and context of the EDPB contribution

The European Data Protection Board (EDPB) very much welcomes the opportunity of the consultation held by the Council of Europe Cybercrime Convention Committee (T-CY) on a draft second additional protocol to the Council of Europe Convention on Cybercrime (Budapest Convention). Such consultation process is even more essential considering that the meetings dedicated to the preparation of the additional protocol are being held in closed sessions and that the direct involvement of data protection authorities in the drafting process has not been foreseen in the T-CY Terms of Reference[1]. The EDPB therefore wishes to provide a constructive and objective contribution with a view to ensure that data protection consideration are duly taken into account in the overall drafting process of the additional protocol.

Access to personal data across jurisdictions has already been addressed in the past by EU data protection authorities in various positions and opinions and the EDPB wishes to recall in particular the Article 29 Working Party's comments on the issue of direct access by third countries' law enforcement authorities to data stored in other jurisdiction, as proposed in the draft elements for an additional protocol to the Budapest Convention on Cybercrime[2], as well as its statement on data protection and privacy aspects of cross-border access to electronic evidence[3]. The European Data Protection Supervisor issued Opinion 03/2019 on the mandate for the participation of the Commission in the negotiations[4], as well as Opinion 7/2019 on proposals regarding European Production and Preservation Orders for electronic evidence in criminal matters[5]. This contribution also builds upon the EDPB Opinion 23/2018 on Commission proposals on European Production and Preservation Orders for electronic evidence in criminal matters[6].

The EDPB acknowledges that situations where judicial and law enforcement authorities are faced with a "cross-border situation" with regards to access to personal data as part of their investigations can be a challenging reality and recognises the legitimate objective of enhancing international cooperation on cybercrime and access to information. In parallel, the EDPB recalls that the protection of personal data and legal certainty must be guaranteed, thus contributing to the objective of establishing sustainable arrangements for the sharing of personal data with third countries for law enforcement purposes, which are fully compatible with the EU Treaties and the Charter of Fundamental Rights. The EDPB furthermore shares the objective of enshrining the preparation of the additional protocol within the framework of the Council of Europe core values and principles, and in particular human rights and the rule of law.

With regards to trans-border direct access to stored computer data as per Article 32(b) of the Budapest Convention, the EDPB reaffirms in particular that data controller can normally only disclose data upon prior presentation of a judicial authorisation/warrant or any document justifying the need to access the data and referring to the relevant legal basis for this access, presented by a national law enforcement authority according to their domestic law that will specify the purpose for which data is required.

As the Cybercrime Convention, as well as any of its additional protocols, is to be considered as a binding international instrument, the EDPB stresses that, in line with the CJEU case law, the "obligations imposed by an international agreement cannot have the effect of prejudicing the constitutional principles of the EC Treaty, which include the principle that all Community acts must respect fundamental rights, that respect constituting a condition of their lawfulness[7]." It is therefore essential that EU negotiating parties ensure that the provisions laid down in the additional protocol do comply with the EU *acquis* in the field of data protection in order to ensure its compatibility with EU primary and secondary law.

[1] Terms of Reference for the Preparation of a Draft 2nd Additional Protocol to the Budapest Convention on Cybercrime, Approved by the 17th Plenary of the T-CY on 8 June 2017, T-CY (2017)3: https://rm.coe.int/terms-of-reference-for-the-preparation-of-a-draft-2nd-additional-proto/168072362b

[2] Article 29 Working Party's comments on the issue of direct access by third countries' law enforcement authorities to data stored in other jurisdiction, as proposed in the draft elements for an additional protocol to the Budapest Convention on Cybercrime, 05/12/2013: https://ec.europa.eu/justice/article-29/documentation/other-document/files/2013/20131205_wp29_letter_to_cybercrime_committee.pdf

[3] WP29 statement on data protection and privacy aspects of cross-border access to electronic evidence, 29 November 2017: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610177

[4] EDPS opinion 3/19 regarding the participation in the negotiations in view of a Second Additional Protocol to the Budapest Cybercrime Convention: https://edps.europa.eu/data-protection/our-work/publications/opinions/budapest-cybercrime-convention_en

[5] EDPS opinion 7/19 on proposals regarding European Production and Preservation Orders for electronic evidence in criminal matters: https://edps.europa.eu/data-protection/our-work/publications/opinions/electronic-evidence-criminal-matters_en

[6] Opinion 23/2018 of the EDPB adopted on 26 September 2018 on Commission proposals on European Production and Preservation Orders for electronic evidence in criminal matters: https://edpb.europa.eu/our-work-tools/our-documents/opinia-art-70/opinion-232018-commission-proposals-european-production_en

[7] See CJEU joined cases C-402/05 P and C-415/05 P, Kadi v. Council, ECLI:EU:C:2008:461 - par (285).

Considering the timeframe of the consultation process, this EDPB contribution will focus on a preliminary assessment of the provisional texts published on 1st October and in particular the new provisions on direct disclosure of subscriber information and on the giving effect to orders from another Party for expedited production of data. The EDPB understands that dedicated provisions on the protection of personal data are still being discussed and will, in this regard, lay down a series of initial recommendations to be considered by the T-CY. As for previous provisions, the EDPB remains available for further contributions and calls for an early and more proactive involvement of data protection authorities in the preparation of these specific provisions, in order to ensure an optimal understanding and consideration of data protections safeguards.

Provisional text of provisions on direct disclosure of subscriber information and on the giving effect of orders for expedited production of data

The EDPB particularly welcomes the opportunity to comment on the draft procedure that provides for the direct cooperation between the authorities of one Party and a service provider in the territory of another Party to obtain subscriber information, as well as on the ability for the requested party to give effect to received order by compelling a service provider in its territory to produce subscriber information or traffic data in the service provider's possession or control. While such provisions may appear of a mainly procedural nature, they are essential in determining the conditions for access to personal data and therefore in assessing a possible interference with the right to the protection of personal data as guaranteed by Article 7 of the Charter of Fundamental Rights of the Union. On the basis of its preliminary assessment, the EDPB recommends further examining the draft provisions with regard to the following elements.

Systematic involvement of judicial authorities of the requested party

The EDPB welcomes the possibility, as per Article 4(5), for a Party to require that an order issued to a service provider in its territory is simultaneously notified to its authorities and that the designated authority may instruct the service provider not to disclose the information if conditions or grounds for refusal would apply under Articles 25.4 and 27.4 of the Convention. However, such safeguard remains at the discretion of each Party to the Convention. As far as EU Parties are concerned, the EDPB stresses that safeguards and limitations affecting the procedural conditions for access to personal data will have to be applied consistently in order to ensure a harmonised level of protection for all persons in the Union.

Article 4(5) does not specifically mention to which type of authority in the requested State orders are to be notified and possibly reviewed. The EDPB recommends that further requirements are included in order to ensure that judicial authorities designated by the authorities of the service provider are involved as early as possible in the process of gathering subscriber information in order to give these authorities the possibility to effectively review compliance of the orders with the Convention and ensure the obligation for these authorities

to raise grounds for refusal on that basis. In this regard, the EDPB recalls that in its case law concerning access to communications data for law enforcement purposes, the CJEU has restricted the possibility to provide for such access, among other criteria, and "except in cases of validly established urgency"[8], to a "prior review carried out by a court or an independent administrative body", "following a reasoned request of [competent national] authorities submitted within the framework of procedures of prevention, detection or criminal prosecution."[9]

The systematic involvement of judicial authorities in the requested parties is also essential to preserve the application of the principle of dual criminality in the field of judicial cooperation. The EDPB recalls that the dual criminality principle aims at providing an additional safeguard to ensure that a State cannot rely on the assistance of another to apply a criminal sanction which does not exist in the law of another State.

Limitation to the status of requesting authority

The EDPB notes and welcomes that, according to Article 4, paragraph 2b, only the requested Party, via a declaration, can impose that the requesting authority is a prosecutor, a judicial authority or another independent authority. However, this could imply, *a contrario* and in the absence of such declaration, that where the requested State did not make such a declaration, orders to service providers could be issued by any authority in the requesting Party. Due to the direct effect of the additional protocol to the Convention in the EU legal order, the draft provisions could then be interpreted as allowing any authority to issue an order, thus putting the lawfulness of the agreement into question in light of EU law. In light of the CJEU case law already cited, the EDPB considers that the type of requesting authorities who may issue such order should be limited to prosecutor, a judicial authority or another independent authority.

Categories of data, definition of "subscriber information" and type of offence

The EDPB recommends that the definition of subscriber information, as per Article 18.3 of the Convention, be further clarified in order to avoid inclusion of any traffic data or content data. Information needed for the purpose of identifying a subscriber of a service may indeed include certain Internet Protocol (IP) address information – for example, the IP address used at the time when an account was created, the most recent log-on IP address or the log-on IP addresses used at a specific time, which under EU law constitute traffic data relating to the transmission of a communication. In addition, the EDPB recalls that, in accordance with the relevant CJEU case law, to establish the existence of an interference with the fundamental right to privacy, it does not matter whether the information on the private lives concerned is sensitive or whether the persons concerned have been inconvenienced in any way. The CJEU has furthermore ruled in its judgement in joined cases C-203/15 and C-698/15 Tele2 Sverige AB that metadata such as traffic data and location data provides the means of establishing a profile of the individuals concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications[10].

[8] See CJEU joint cases C-203/15 and C-698/15, Tele2 Sverige AB, ECLI:EU:C:2016:970 – par (120)
[9] See CJEU joint cases C-293/12 and C-594/12, Digital Rights Ireland Ltd, ECLI:EU:C:2014:238 – par (62)
[10] See CJEU joint cases C-203/15 and C-698/15, Tele2 Sverige AB, ECLI:EU:C:2016:970 – par (99)

The EDPB also takes the view that the balance between the types of offences for which an Order can be issued and the categories of data concerned shall be reassessed in order to limit the possibility to submit an Order to produce data that could be considered as traffic data, to serious crimes only. Furthermore, the definition of a common list of specific serious criminal offences should be further explored.

Security of data processing

Although Article 4(6) and Article 5(5) provide that appropriate levels of security and authentication may be required, the EDPB encourages the development of further specifications and requirements in this regard. Ensuring that the necessary means are put in place so that the personal data are disclosed and communicated in a secure environment with the means to ensure the authenticity of documents is key for achieving the objective of a swift gathering of electronic evidence in compliance with fundamental rights.

In relation to the security of data processing, the EDPB also invites the T-CY to consider, as a specific data protection safeguard, a mechanism for the notification without delay of data breaches that could seriously interfere with the rights and freedoms of data subjects. Personal data breaches could indeed potentially have a range of significant adverse effects for individuals concerned.

Provisions on data protection safeguards

The EDPB considers essential that the provisional text submitted to public consultation is complemented by dedicated provisions on data protection safeguards, which must then be assessed together in order to ensure the draft additional protocol translates into a sustainable arrangement for the sharing of personal data with third countries for law enforcement purposes, fully compatible with the EU Treaties and the Charter of Fundamental Rights.

Provisional text of provisions on direct disclosure of subscriber information and on the giving effect to orders from another Party for expedited production of data, by laying down procedural conditions for access to personal data, may already impact on the level of protection of personal data and may also need to be amended in order to ensure the operational application of appropriate data protection safeguards.

The EDPB considers that specific provisions on data protection safeguards shall reflect key principles and in particular lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality. These principles are also in line with the Council of Europe modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Convention 108+), to which many Parties to the Convention on Cybercrime are also Party.

Substantive and procedural conditions for access to personal data

As stated by the Article 29 Working Party on data protection and privacy aspects of cross-border access to electronic evidence, the EDPB recalls that the current EU legal framework and the most recent case law can allow the development of a list of substantive and procedural conditions to be taken into account for any future instrument governing law enforcement access to personal data. Considering the direct effect of an additional protocol to the Convention in the EU legal order, the following conditions for access to personal data remain relevant:

- The conditions under which the providers of electronic communications services must grant such access must be provided by law, so as to ensure that the processing relies on a clear legal basis.
- Individual access can, as a general rule, be granted, in relation to the objective of fighting crime, only to the data of individuals suspected of planning, committing or having committed a serious crime or of being implicated in one way or another in such a crime.
- Access of the competent national authorities to data should, as a general rule, except in cases of validly established urgency, be subject to a prior review carried out either by a court or by an independent administrative body.
- In particular situations, where for example national security, defence or public security interests are threatened by terrorist activities, access to the data of other persons might also be granted where there is objective evidence from which it can be deduced that that data might, in a specific case, make an effective contribution to combating such activities.
- Personal data collected should be adequate, relevant and not excessive for the purpose of the processing.
- The processing of special categories of personal data should be subject to further limitations and safeguards.
- The competent national authorities to whom access to the data has been granted must notify the persons affected, under the applicable national procedures, as soon as that notification is no longer liable to jeopardize the investigations being undertaken by those authorities.
- Personal data should be correct, up to date and should not be kept longer than necessary.
- Notification is necessary to enable the persons affected to exercise, inter alia, their right to a legal remedy and their data protection rights in relation to the processing of their data.

Availability of effective legal remedies

The EDPB also considers of paramount importance that the additional protocol includes mechanism to ensure the availability of legal remedies to the data subject whose data has been obtained, at least equivalent to those available in a domestic case. In this regard, the EDPB recalls that the CJEU has stated that "the first paragraph of Article 47 of the Charter requires everyone whose rights and freedoms guaranteed by the law of the European Union are violated to have the right to an effective remedy before a tribunal in compliance with the conditions laid down in that article. The very existence of effective judicial review designed to ensure compliance with provisions of EU law is inherent in the existence of the rule of law"[11].

[11] See CJEU C-362/14, Maximillian Schrems, ECLI:EU:C:2015:650 – par (95)

Further processing and onward transfer

The EDPB highlights that published provisional texts do not contain any specific limit with regard to the further processing and onward transfers of the transferred personal data by the requesting Party authority. The EDPB therefore recommends specifying narrowly the purposes of the transfers and the prohibition of further processing incompatible with those purposes and including the general principle of prohibition of onward transfers unless the third country provides an appropriate level of protection, in order to prevent the level of protection provided for in the protocol from being circumvented by further processing and onward transfers of personal data to other third countries.

Oversight and monitoring mechanism

In light of the comments and recommendations above, the EDPB finally invites the T-CY to consider the development of a mechanism for the oversight and monitoring by an independent authority, with both investigatory and corrective enforcement powers, responsible to ensure the application of future data protection safeguards in practice.

The EDPB reiterates the importance of involving data protection authorities in the drafting process of the additional protocol and stands ready to contribute and assist the T-CY in the preparation of provisional text of provisions on data protection safeguards.



EDPB oral pleading before the Court of Justice of the EU

Case C-311/18 (Facebook Ireland and Schrems)

9th July 2019, 9h00

Luxembourg

With regard to the first question on standard contractual clauses (SCCs):

- The SCCs adopted by the COM are instruments with a general scope. They are not related to any specific third country. They are provided for an individual transfer contract from an EU-exporter to a third country importer.
- Therefore, the EDPB considers that the COM is not obliged to examine whether the access of the public authorities of a given third country to the data transferred respects the level of protection required by EU law.
- The EDPB considers that this is primarily the responsibility of the exporter and the importer, when considering whether to enter into the SCCs.
- This means that it is also for SAs, in particular on the basis of a complaint, to assess whether the continuity of the protection afforded by Union law is ensured once the data were transferred, including whether the

exporter and importer complied with their obligations under the SCCs. If not, SAs may suspend transfers.

- Under SCCs, SAs are only empowered to assess individual cases but do not have the power to issue a general ban of transfers to a specific third country.

As far as the second question is concerned, on data during the stage of transit:

- On the first part of the question: The EDPB takes the view that the continuity of the protection afforded under EU laws needs to be ensured, also during the stage of transit to a third country, no matter which transfer tool is used.
- In the context of an assessment of adequacy, when assessing the level of protection of the laws of a third country the EDPB has stated that COM's analysis should not be limited to the law and practice allowing for surveillance within that country's physical borders. It should also cover the law and practice allowing for surveillance outside or on its way to its physical borders, as far as EU data are concerned.
- The EDPB takes the view that, no matter which Chapter V GDPR transfer tool is used, the assessment should be limited to applicable laws and practices in the third country where the recipient is. The EDPB sees no obligation to assess any other country's laws which could provide for the possibility to intercept data on their way to the third country where the recipient is.
- With regard to the U.S., the EDPB included the Executive Order 12333, which applies to the collection of data by the U.S. authorities outside the U.S. territory, and the Presidential Policy Directive 28 (PPD-28), when commenting on the Privacy Shield decision and its joint reviews.
- On the second part of the question: the adoption of an adequacy decision may create a presumption, if the respect for the level of protection during the stage of transit was made part of the adequacy finding.
- Though the EDPB notes that reference is made to data in transit in the Privacy Shield adequacy decision, the level of protection during the stage of transit was not discussed during both Privacy Shield Joint Reviews, as the U.S. Government stated that the stage of transit is not covered by the Privacy Shield.

In relation to the third question on the level of protection required:

- The EDPB takes the view that, in order to assess the legal framework of a third country, all domestic rules should be taken into account when making an assessment of adequacy. This includes the limits within which the administration of that third country may collect data, as long as those domestic rules are publicly available, sufficiently clear and precise, and binding on the administration.
- At the same time, the EDPB would like to stress that the level of protection in the third country can only be ensured by laws of the third country which confer enforceable and effective rights on the data subject and which can be relied on before courts or tribunals.

With reference to the fourth question, on access to personal data by a public authority:

- In our view, as the screening of communications and access to data in this context are inextricably linked to the process of collection of data, the access to data by means of selectors for the purposes of screening communications is part of the processing of the data collected.
- I would like to refer to the specific context of the Privacy Shield, in particular with regard to US programmes run under the authority of 702 FISA, which aim at collecting personal data by means of selectors following the screening of communications. The EDPB, in its reports on the 1st and 2nd Joint Reviews of the Privacy Shield, stressed the importance of more specific safeguards for these measures, for example for precise targeting to determine whether an individual or a group can be a target of surveillance, and for strict scrutiny of individual targets by an independent authority ex-ante.

Regarding the fifth question, on the Privacy Shield Ombudsperson:

- The EDPB welcomed the establishment of the Ombudsperson mechanism as a new redress mechanism.
- At the same time, the EDPB expressed concern with regard to effective judicial redress before the courts of the U.S., and examined if the Ombudsperson mechanism could have offset these deficiencies with respect to individual judicial protection. The EDPB took the view that the Ombudsperson mechanism could only offset the deficiencies of judicial redress if the requirements of Art. 47 of the Charter are met.
- The EDPB thus focused on the question how independent the Ombudsperson is and what powers she/he has.
- The EDPB stated in the last Privacy Shield joint review issued earlier this year that it is not in a position to conclude that the Ombudsperson is vested with sufficient powers to access information and to remedy non-compliance. The EDPB went on to say it can thus not state that the Ombudsperson can be considered an "effective remedy before a tribunal" in the meaning of Art. 47 of the Charter of Fundamental Rights.

In relation to the sixth question, on the US Government's replies:

- The EDPB refrains from commenting on the replies by the United States Government.

Finally, I would like to make some additional remarks:

- Personal data of Europeans are well protected through the high European standards provided and enshrined in the Charter of Fundamental Rights and the GDPR.
- As one of the judges of this court said after the Schrems I ruling, this protection "is sailing with the data, wherever the data are transferred to".
- We, the SAs, used our powers and capacities to uphold this standard and to spread it, bearing in mind consideration 42 of the Schrems I ruling

stating "*that national SA must in particular ensure a fair balance between, on the one hand, observance of the fundamental right to privacy and on the other hand, the interests requiring free movement of personal data*", and recital 4 of the GDPR.

Andrea Jelinek

Chair of the European Data Protection Board



Information note on data transfers under the GDPR to the United Kingdom after the transition period

Adopted on 15 December 2020

The transition period for the United Kingdom's withdrawal from the European Union will end on 31 December 2020. This means that as of 1 January 2021, the UK will no longer apply the GDPR to the processing of personal data and a separate legal framework regarding data protection will be in force in the UK. Consequently, as of 1 January 2021, all transfers of personal data between stakeholders subject to GDPR and UK entities will constitute a transfer of personal data to a third country and therefore will be subject to the provisions of Chapter V GDPR.

In the absence of an adequacy decision applicable to the UK as per Article 45 GDPR, such transfers will require appropriate safeguards (e.g., standard data protection clauses, binding corporate rules[1], codes of conduct…), as well as enforceable data subject rights and effective legal remedies for data subjects, in accordance with Article 46 GDPR.

Subject to specific conditions, it may still be possible to transfer personal data to the UK based on a derogation listed in Article 49 GDPR. However, Article 49 GDPR has an exceptional nature and the derogations it contains must be interpreted restrictively and mainly relate to processing activities that are occasional and non-repetitive[2].

Moreover, where personal data are transferred to the UK on the basis of Article 46 GDPR safeguards, supplementary measures might be necessary to bring the level of protection of the data transferred up to the EU standard of essential equivalence, in accordance with the Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data[3].

[1] See EDPB information note on BCRs for Groups of undertakings / enterprises which have ICO as BCR Lead SA, https://edpb.europa.eu/our-work-tools/our-documents/other/information-note-bcrs-groups-undertakings-enterprises-which-have_en

[2] See Guidelines 02/2018 on derogations of Article 49 under Regulation 2016/679, https://edpb.europa.eu/our-work-tools/our-documents/directrices/guidelines-22018-derogations-article-49-under-regulation_en

[3] See Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer_en

Controllers and/or processors will also need to comply with other obligations deriving from the GDPR, in particular on the need to update the records of processing and privacy notices to mention transfers to the UK.

The EDPB recalls the guidance provided on this matter by supervisory authorities and by the European Commission (EC). EEA organisations may turn, if necessary, to the national supervisory authorities competent to oversee the related processing activities.

For data transfers from the UK to the EEA, the EDPB would suggest regularly consulting the UK Government's website and the ICO's website for up-to-date guidance.

For the European Data Protection Board

The Chair

(Andrea Jelinek)



W sytuacji gdyby Zjednoczonego Królestwo wyszło z UE bez porozumienia, a ICO przestanie być jednym z organów nadzorczych właściwych w sprawach dotyczących wiążących reguł korporacyjnych (BCR), przedsiębiorstwa powinny wziąć pod uwagę poniższe:

• Grupy z siedzibą w Zjednoczonym Królestwie, które chcą złożyć wniosek o zatwierdzenie BCR: grupy takie powinny określić najbardziej odpowiedni wiodący organ nadzorczy w sprawie dotyczącej BCR w państwie członkowskim UE, zgodnie z kryteriami określonymi w pkt. 1.2 dokumentu WP 263.

• Obecnie rozpatrywanie wnioski: Grupy, dla których BCR są na etapie rozpatrywania przez ICO, muszą określić wiodący organ nadzorczy w sprawie dotyczącej BCR zgodnie z kryteriami określonymi w WP 263. Nowy wiodący organ nadzorczy w sprawie dotyczącej BCR przejmie wniosek i z chwilą wyjścia Zjednoczonego Królestwa z UE bez porozumienia formalnie rozpocznie nową procedurę.

Projekty BCR przedłożone EROD: jeśli w chwili wyjścia Zjednoczonego Królestwa z UE bez porozumienia projekt decyzji ICO zatwierdzającej BCR będzie w trakcie rozpatrywania przez EROD, grupa musi wyznaczyć nowy wiodący organ nadzorczy w sprawie dotyczącej BCR zgodnie z kryteriami określonymi w dokumencie WP 263. Nowy wiodący organ nadzorczy w sprawie dotyczącej BCR przejmie i ponownie przedłoży EROD projekt decyzji w celu zatwierdzenia EROD.

• Podmioty z zatwierdzonymi BCR: Podmioty z już zatwierdzonymi BCR powinny określić nowy wiodący organ nadzorczy w sprawie dotyczącej BCR zgodnie z kryteriami określonymi w dokumencie WP 263.

W każdym z powyższych scenariuszy organ nadzorczy będący potencjalnym nowym wiodącym organem nadzorczym w sprawie dotyczącej BCR rozważy w poszczególnych przypadkach i we współpracy z innymi zainteresowanymi organami nadzorczymi, czy jest właściwym wiodącym organem nadzorczym w sprawie dotyczącej BCR, i poinformuje grupę o swojej decyzji. W przypadku pytań lub próśb o dalsze informacje grupy są proszone o skontaktowanie się z ICO.

W imieniu Europejskiej Rady Ochrony Danych

Przewodnicząca

(Andrea Jelinek)



Nota informacyjna dotycząca przekazywania danych osobowych na podstawie ogólnego rozporządzenia o ochronie danych w przypadku braku porozumienia w sprawie brexitu

Przyjęta 12 lutego 2019 r.
Zaktualizowana: 4 października 2019 r.

Wprowadzenie

W przypadku braku porozumienia między EOG a Zjednoczonym Królestwem (scenariusz braku porozumienia w sprawie brexitu), Zjednoczone Królestwo stanie się państwem trzecim w dniu 1 listopada 2019 r. od godz. 00:00 czasu środkowoeuropejskiego. Oznacza to, że z dniem 1 listopada 2019 r. przekazywanie danych osobowych do Zjednoczonego Królestwa musi opierać się na jednym z następujących instrumentów[1]:

- klauzule ochrony danych - standardowe lub ad hoc
- wiążące reguły korporacyjne
- kodeksy postępowania i mechanizmy certyfikacji
- wyjątki[2]

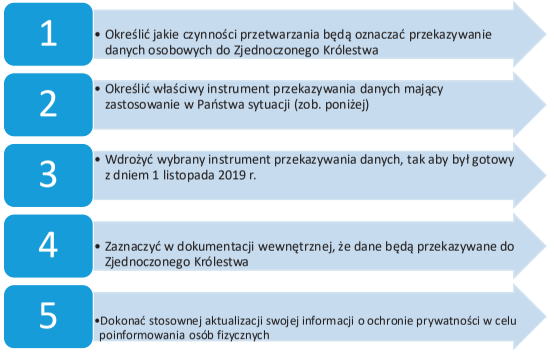
Niniejsza nota zawiera informacje dla organizacji komercyjnych i publicznych dotyczące tych instrumentów przekazywania danych przewidzianych w ogólnym rozporządzeniu o ochronie danych, które znajdą zastosowanie do przekazywania danych osobowych do Zjednoczonego Królestwa w przypadku braku porozumienia w sprawie brexitu.

Europejska Rada Ochrony Danych (EROD) opiera się na wytycznych przedstawionych w tej sprawie przez organy nadzorcze oraz Komisję Europejską (KE). Organizacje EOG mogą, w razie konieczności, zwrócić się do krajowych organów nadzorczych właściwych do nadzorowania powiązanych czynności przetwarzania.

1 Zobacz Rozdział V RODO.
2 Mają one zastosowanie jedynie w przypadku braku standardowych klauzul ochrony danych lub innych stosownych alternatywnych zabezpieczeń.

I. Pięć kroków, jakie organizacje powinny podjąć w celu przygotowania się na scenariusz braku porozumienia w sprawie brexitu

Przekazując dane do Zjednoczonego Królestwa, należy:



II. Przekazywanie danych z EOG do Zjednoczonego Królestwa

1. *Dostępne instrumenty przekazywania danych*

W przypadku braku decyzji stwierdzającej odpowiedni poziom ochrony danych osobowych[3] w momencie brexitu dostępne będą następujące instrumenty przekazywania danych.

a. Klauzule ochrony danych - standardowe i ad hoc

Państwo oraz Państwa partner ze Zjednoczonego Królestwa możecie zgodzić się na zastosowanie standardowych klauzul ochrony danych zatwierdzonych przez Komisję Europejską. Zapewniają one dodatkowe odpowiednie zabezpieczenia w odniesieniu do ochrony danych, które są potrzebne w przypadku przekazywania danych osobowych do dowolnego państwa trzeciego.

[3] Decyzja stwierdzająca odpowiedni stopień ochrony danych osobowych to decyzja przyjęta przez Komisję Europejską na podstawie art. 45 RODO (na przykład, decyzja stwierdzająca odpowiedni stopień ochrony w Japonii przyjęta przez Komisję w dniu 23 stycznia 2019 r. Poprzednio KE przyjęła również decyzje stwierdzające odpowiedni stopień ochrony w państwach trzecich takich jak m.in. Argentyna, Nowa Zelandia i Izrael). Obecnie taka decyzja stwierdzająca odpowiedni stopień ochrony nie istnieje w stosunku do Zjednoczonego Królestwa.

Obecnie dostępne są trzy zestawy standardowych klauzul ochrony danych:

- administrator danych z EOG do administratora danych z państwa trzeciego (np. ze Zjednoczonego Królestwa): dostępne są dwa zestawy:
  - 2001/497/WE
  - 2004/915/WE
- administrator danych z EOG do podmiotu przetwarzającego dane z państwa trzeciego (np. ze Zjednoczonego Królestwa)
  - 2010/87/WE

Należy zauważyć, że standardowe klauzule ochrony danych nie mogą być zmieniane i muszą być podpisane w przewidzianej formie. Mogą być one jednak zawarte w szerszej umowie, a dodatkowe klauzule mogą być dodawane, pod warunkiem że nie są one bezpośrednio lub pośrednio sprzeczne ze standardowymi klauzulami ochrony danych przyjętymi przez Komisję Europejską. Biorąc pod uwagę ramy czasowe do dnia 1 listopada 2019 r., EROD uznaje, że standardowe klauzule ochrony danych stanowią instrument gotowy do użycia.

Wszelkie dalsze zmiany w standardowych klauzulach ochrony danych oznaczają, że zostaną one uznane za klauzule umowne ad-hoc. Może to zapewnić odpowiednie zabezpieczenia uwzględniające Państwa konkretną sytuację.

Przed jakimkolwiek przekazaniem danych te dostosowane do konkretnej sytuacji klauzule umowne muszą zostać zatwierdzone przez właściwy krajowy organ nadzorczy po uzyskaniu opinii Europejskiej Rady Ochrony Danych (EROD).

b. Wiążące reguły korporacyjne

Wiążące reguły korporacyjne to polityki ochrony danych osobowych, których przestrzegają grupy przedsiębiorstw (tj. przedsiębiorstwa międzynarodowe) w celu zapewnienia odpowiednich zabezpieczeń w odniesieniu do przekazywania danych osobowych w ramach grupy, w tym poza EOG.

Mogą Państwo stosować już wiążące reguły korporacyjne lub współpracować z podmiotami przetwarzającymi, które stosują wiążące reguły korporacyjne dla podmiotów przetwarzających. Organizacje mogą nadal opierać się na tych wiążących regułach korporacyjnych zatwierdzonych na podstawie poprzedniej dyrektywy 95/46/WE, które zachowują ważność na mocy ogólnego rozporządzenia o ochronie danych[4]. Należy jednak zaktualizować te wiążące reguły korporacyjne, aby były one w pełni zgodne z przepisami ogólnego rozporządzenia o ochronie danych (RODO).

Jeżeli nie posiadają Państwo wiążących reguł korporacyjnych, muszą one zostać zatwierdzone przez właściwy krajowy organ nadzorczy po uzyskaniu opinii Europejskiej Rady Ochrony Danych.

Więcej informacji na temat warunków ubiegania się o wiążące reguły korporacyjne można znaleźć na stronie internetowej EROD.

[4] Zgodnie z art. 46. ust.5 RODO. Należy zwrócić uwagę, że wiążące reguły korporacyjne zatwierdzone na podstawie poprzedniej dyrektywy 95/46/WE zachowały ważność na mocy ogólnego rozporządzenia o ochronie danych, ale należy je zaktualizować, aby były w pełni zgodne z przepisami ogólnego rozporządzenia o ochronie danych (RODO).

c. Kodeksy postępowania i mechanizmy certyfikacji

Kodeks postępowania lub mechanizm certyfikacji mogą oferować odpowiednie zabezpieczenia dla przekazywania danych osobowych, jeżeli zawierają wiążące i egzekwowalne zobowiązania organizacji w państwie trzecim na rzecz osób fizycznych.

Narzędzia te są nowe na mocy ogólnego rozporządzenia o ochronie danych, a Europejska Rada Ochrony Danych pracuje nad wytycznymi w celu zapewnienia dokładniejszych wyjaśnień dotyczących zharmonizowanych warunków i procedur stosowania tych narzędzi.

2. *Wyjątki*

Należy podkreślić, że wyjątki zezwalają na przekazywanie danych pod pewnymi warunkami i są wyjątkami od zasady wprowadzenia odpowiednich zabezpieczeń (zob. wyżej wymienione instrumenty, takie jak wiążące reguły korporacyjne, standardowe klauzule ochrony danych itp.) lub przekazują dane na podstawie decyzji stwierdzającej odpowiedni stopień ochrony danych osobowych. Dlatego muszą być one interpretowane w sposób zawężający i odnosić się głównie do czynności przetwarzania, które są sporadyczne i niepowtarzające się[5].

Zgodnie z art. 49 RODO wyjątki te obejmują między innymi:

- sytuację, w której osoba fizyczna, po otrzymaniu wszelkich niezbędnych informacji na temat ryzyka związanego z takim przekazaniem, wyraźnie wyraziła na nie zgodę;
- sytuację, w której przekazanie jest niezbędne do wykonania lub zawarcia umowy między osobą fizyczną a administratorem danych lub umowa zostaje zawarta w interesie osoby fizycznej;
- sytuację, w której przekazanie jest niezbędne ze względu na ważne względy interesu publicznego;
- sytuację, w której przekazanie jest niezbędne ze względu na ważne prawnie uzasadnione interesy organizacji.

Więcej informacji na temat dostępnych wyjątków oraz o sposobie ich zastosowania można znaleźć w wytycznych Europejskiej Rady Ochrony Danych dotyczących art. 49 ogólnego rozporządzenia o ochronie danych.

3. *Instrumenty dostępne wyłącznie dla organów lub podmiotów publicznych*

Organy publiczne mogą rozważyć wykorzystanie mechanizmów, które zgodnie z ogólnym rozporządzeniem o ochronie danych bardziej odpowiadają ich sytuacji.

Jedną z możliwości jest zastosowanie prawnie wiążącego i egzekwowalnego instrumentu, takiego jak porozumienie administracyjne, dwustronne lub wielostronne porozumienie międzynarodowe. Porozumienie musi być wiążące i egzekwowalne w odniesieniu do sygnatariuszy.

5 Zobacz motyw 113 i art. 49. ust. 1 RODO

Druga możliwość polega na stosowaniu uzgodnień administracyjnych, takich jak protokoły ustaleń, które mimo że nie są prawnie wiążące, muszą jednak przewidywać egzekwowalne i skuteczne prawa osób, których dane dotyczą. Ustalenia administracyjne podlegają zatwierdzeniu przez właściwy krajowy organ nadzorczy po wydaniu opinii przez Europejską Radę Ochrony Danych.

Ponadto wspomniane wyżej wyjątki są również dostępne w odniesieniu do przekazywania danych dokonanego przez organy publiczne, z zastrzeżeniem zastosowania odpowiednich warunków.

W przypadku organów publicznych pełniących funkcje w zakresie egzekwowania prawa karnego[6], dostępne są dodatkowe narzędzia przekazywania danych[7].

III. Przekazywanie danych ze Zjednoczonego Królestwa do państw członkowskich EOG

Według rządu Zjednoczonego Królestwa obecne praktyki, które umożliwiają swobodny przepływ danych osobowych ze Zjednoczonego Królestwa do EOG, będą kontynuowane w przypadku braku porozumienia w sprawie brexitu[8].

W tym celu należy regularnie zapoznawać się z treścią strony internetowej rządu Zjednoczonego Królestwa oraz Biura Rzecznika ds. Informacji (ICO).

W imieniu Europejskiej Rady Ochrony Danych
Przewodnicząca

(Andrea Jelinek)

6 Które wchodzą w zakres dyrektywy w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar oraz w sprawie swobodnego przepływu takich danych (tzw. dyrektywy policyjnej

7 Zobacz art. 37 i 38 dyrektywy policyjnej. Na przykład przekazanie danych może mieć miejsce jeśli organ UE uzna, iż w państwie trzecim istnieją odpowiednie zabezpieczenia po przeprowadzeniu (własnej) oceny wszystkich okoliczności dotyczących takiego przekazania danych. Ponadto w szczególnych przypadkach mogą mieć zastosowanie dodatkowe wyjątki (zob. art. 38 dyrektywy policyjnej).

8 https://www.gov.uk/government/publications/data-protection-if-theres-no-brexit-deal/data-protection-if-theres-no-brexit-deal



EU - U.S. Privacy Shield - Second Annual Joint Review

Adopted on 22 January 2019

Table of contents

1 Executive summary 4
1.1 Introduction 4
1.2 On the commercial aspects of the Privacy Shield 4
1.3 On the access by public authorities to data transferred to the U.S. under the Privacy Shield 6
1.4 Conclusion 7
2 Introduction 8
3 On the commercial aspects of the Privacy Shield 9
3.1 Guidance for the companies adhering to the Privacy Shield 9
3.2 Clear and easily available information for EU individuals 10
3.3 Self-(Re)Certification Process and Cooperation between U.S. authorities in the Privacy Shield mechanism 10
3.4 Oversight and supervision of compliance with the Principles – Activities of the DoC 12
3.5 Oversight and supervision of compliance with the Principles – Activities of the FTC 13
3.6 Independent Recourse Mechanisms 13
3.7 HR Data 14
3.8 Automated-decision making/Profiling 14
4 On the derogations to the Privacy Shield to allow access to data for Law Enforcement and National Security purposes 16
4.1 Introduction 16
4.2 Collection of data (under section 702 and under EO 12333) 16
4.2.1 Collection of data for national security purposes under Section 702 16
4.2.2 Collection of data for national security purposes under Executive Order 12333 17
4.3 Oversight 17
4.4 Redress for EU individuals 18
4.5 Ombudsperson mechanism 19
4.6 Access to data for law enforcement purposes 20
5 Conclusion 20
ANNEX TO THE EDPB REPORT ON THE SECOND EU-US PRIVACY SHIELD ANNUAL JOINT REVIEW 22
General Information 22
1 On commercial aspects 22
1.1 Self-Certification Process and Cooperation between U.S. authorities in the Privacy Shield Program 22
1.2 Oversight and supervision of compliance with the principles - Activities by the DoC 23
1.3 Oversight and supervision of compliance with the principles - Activities by the FTC 24

1.4 Oversight and supervision of compliance with the principles - Activities by the DoT 25
1.5 Guidance for the companies adhering to the Privacy Shield 25
1.6 IRM 25
1.7 Arbitral Panel 25
1.8 Automated Decision Making 25
1.9 HR Data 26
2 On government access to personal data: relevant developments in the U.S. legal framework and trends 27
2.1 Reauthorisation of 702 FISA 27
2.2 PPD-28 27
2.3 The Ombudsperson mechanism and the EU individual complaint handling body 27
2.4 PCLOB 28
2.5 Inspector General (IG) of the ODNI 28
2.6 Redress 28
2.7 Additional information on access to data by law enforcement authorities 29

The European Data Protection Board

Having regard to Article 4 and Recitals 145 to 149 of the Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield ("EU - U.S. Privacy Shield),

HAS ADOPTED THE FOLLOWING REPORT:

1 EXECUTIVE SUMMARY

1.1 Introduction

1. According to the EU–U.S. Privacy Shield adequacy decision ("Privacy Shield")[1] adopted on 12 July 2016, **seven representatives of the EDPB participated in the second joint review conducted by the European Commission, on October 18 and 19 of 2018** in Brussels to assess the robustness of its adequacy decision and its practical implementation.
2. Based on the concerns elaborated in the previous opinions of the WP29, in particular opinion 1/2016, and in its report following the first joint review, the EDPB focused on the assessment of both the **commercial aspects** of the Privacy Shield and on the **government access to personal data transferred from the EU for the purposes of Law Enforcement and National Security, including the legal remedies available to EU citizens**, The EDPB assessed once again whether these concerns have been addressed and also whether the safeguards provided under the EU-U.S. Privacy Shield are workable and effective.
3. The European Commission published its report of the second joint review on December 19, 2018.
4. **The EDPB's main findings concerning this second joint annual review**, stemming both from written submissions and from oral contributions are hereby presented in this report.

1.2 On the commercial aspects of the Privacy Shield

5. The second annual review showed that **many of the WP 29's findings of the first annual review regarding the commercial aspects have been taken into account by the US authorities**. The EDPB acknowledges that on the commercial aspects significant progress has been made especially with regards to the following aspects.
6. The **DoC has adapted the initial certification process** in a way that the inconsistencies between the Privacy Shield List and the representations made by the organizations regarding their participation in the Privacy Shield program on their websites are now avoided as far as the initial certification process is concerned.
7. The **DoC as well as the FTC have started to also take ex officio oversight and enforcement actions as regards the compliance of Privacy Shield certified organizations** with the requirements under the Privacy Shield.

[1] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, OJ L 207, 1.8.2016, p.1.

8. The **DoC has issued further guidance for the EU individuals** in order to facilitate their understanding of the Privacy Shield and the exercise of their rights. The **DoC has also started to issue further guidance for the U.S. Businesses** in order to clarify the requirements of the Privacy Shield. The EDPB still expects this guidance will provide the necessary clarifications to facilitate the proper application, and where necessary will be adjusted.

9. **However, one of the main concerns already expressed by the WP29 remains a certain lack of oversight in substance**. Indeed, the checks performed by the DoC are principally focused on formal aspects. The enforcement actions by the FTC could not be fully assessed during the review, since the FTC was not able to share substantial information on the subject matter of the new ex officio enforcement actions taken. **This lack of substantial checks thus remains a concern of the EDPB as, even taking into account discretionary and limited investigations by the FTC, a majority of companies' compliance with the substance of the Privacy Shield's principles remains unchecked**. The Privacy Shield presents in its Annex 1 "the clarification that Privacy Shield organizations must limit personal information to the information that is relevant for the purposes of processing" as an enhancement of the Privacy Shield. This is only one example for many substantial requirements set out by the Privacy Shield whose correct application has to be ascertained through sufficient oversight and enforcement action by the competent U.S. authorities.

10. **Another issue where the EDPB sees further need to work on concern the area of onward transfers**. Since onward transfers possibly lead to transfers of data outside of the jurisdiction of U.S. and EU authorities with possibly no data protection provided by law it is of utmost importance that the competent US Authorities closely monitor the practical implementation of the Privacy Shield's "Accountability for the Onward Transfers Principle". As a first step, for example the DoC could make use of its right to ask organizations to produce the contracts they have put in place with third countries' partners in order to assess whether those provide the necessary safeguards and to discover if any further guidance or other action by the DoC or the FTC is needed.

11. **Another area that requires further attention is the application of the Privacy Shield requirements regarding HR Data**. While the EU Supervisory authorities remain available to exchange with the US Authorities, the discussions on this issue will have to continue between the European Commission and the US Authorities given the different possible readings of the wording of the Privacy Shield. In parallel, the Commission is still called upon to address this issue and clarify the text in order to avoid that possible different interpretations do not lead to gaps in the protection of EU data subjects.

12. **Also, the re-certification process needs to be further refined**. The situation of outdated listings leads to avoidable confusion that should be addressed also in the interest of concerned Privacy Shield certified organizations.

13. Last but not least, the EDPB recalls the **remaining issues** with respect to certain elements of the commercial part of the Privacy Shield adequacy decision as already raised in the WP 29's Opinion 01/2016 in particular regarding the absence or the limitation to the rights of the data subjects (i.e. right to object, right to access, right to be informed for HR processing), the absence of key definitions, the lack of guarantees on transfers for regulatory purpose in the field of medical context, the lack of specific rules on automated decision making and the overly broad exemption for publicly available information. Those remain valid.

1.3 On the access by public authorities to data transferred to the U.S. under the Privacy Shield

14. The EDPB **welcomes the appointments of three new members of the Privacy and Civil Liberties Oversight Board (PCLOB), including its Chair, enabling it to reach the quorum**. It hopes that the two remaining positions will also be filled, which are important to respect the requirement concerning the bipartisanism of the members. The PCLOB is thus in a position again to prepare and issue reports.

15. The EDPB also welcomes the fact that the US authorities have published the report on Presidential Policy Directive 28 (PPD-28), in a redacted form, which mainly clarifies that the PPD-28 is applied by all agencies of the Intelligence Community, and it acknowledges the efforts made by the U.S. government by publishing a number of important documents, for example, decisions by the Foreign Intelligence Surveillance Court (FISA Court), in part by declassification, and the setting up of a new website.

16. Despite these developments, **some of the main points of concern, already expressed by the WP29 in this area in its previous report, still have to be fully resolved**.

17. More specifically, the **collection and access of personal data for national security purposes** under both Section 702 of FISA and Executive Order 12333 still remains an important issue for the EDPB, **especially with regards to massive and indiscriminate access** (on this issue, see in particular the statement of the WP29 on the decision of the European Commission on the EU-U.S. Privacy Shield of 26 July 2016[2]).

18. In this respect, **the EDPB can only encourage the PCLOB to issue further reports**, on PPD-28 to follow up on the first report in order to provide additional elements as to how the safeguards of PPD-28 are applied, as well as a follow-up report on Section 702 FISA. The EDPB recalls that the WP29 considered a report on Section 702 important for assessing whether the collection of data under section 702 is not indiscriminate and access is not conducted on a generalized basis under the UPSTREAM program, and for assessing the necessity and proportionality of the definition of "targets", the tasking of selectors under **section 702** (including in the context of the **UPSTREAM program**), as well as the concrete process of application of selectors in the context of the UPSTREAM program to clarify whether massive access to data occurs in this context.

19. **The EDPB regrets that the reauthorization of Section 702 FISA did not lead to the introduction of any new guarantees for EU individuals**. The EDPB recalls that, in its report following the first annual Joint Review in 2017, the WP29 considered that instead of generally authorizing surveillance programs, more specific safeguards would be needed, e.g. for precise targeting to determine whether an individual or a group can be a target of surveillance and for stricter scrutiny of individual targets by an independent authority ex-ante.

20. Concerning the application of **Executive Order 12 333** to EU data transferred to the U.S., the EDPB would welcome if the PCLOB finalized and issued its awaited report on EO 12 333 to provide information on the concrete operation of this Executive Order and on its necessity and proportionality.

21. The redress by EU citizens before U.S. courts is still to be effectively guaranteed due to the problematic admissibility threshold of the **"standing requirement"**. Therefore, the EDPB will continue to follow closely the evolution of the case law.

[2] https://ec.europa.eu/justice/article-29/press-material/press-release/art29_press_material/2016/20160726_wp29_wp_statement_eu_us_privacy_shield_en.pdf

22. Hence, the independence of the Ombudsperson remains a key element, as this institution is designed to compensate the uncertainty in seeking effective redress before the court, if not the lack thereof. In any case, a permanent Ombudsperson **is still to be appointed**.

23. The exact powers of the Ombudsperson also need to be clarified through the **declassification of internal procedures** concerning the interactions between the Ombudsperson and the other elements of the intelligence community or oversight bodies. Based on the information provided so far, the EDPB is of the view that the powers of the Ombudsperson to remedy non-compliance vis-à-vis the intelligence authorities are still not sufficient in the light of Article 47 EU Charter of Fundamental Rights, and also underlines that the Ombudsperson is not in a position to bring a matter before the court.

24. Finally, regarding the **access to data for law enforcement purposes**, the EDPB underlines its remaining concerns on the available effective remedies for individuals in cases where the personal data processed by companies are accessed by law enforcement authorities.

1.4 Conclusion

25. The EDPB **welcomes the efforts made by the U.S. authorities and the Commission to implement the Privacy Shield, especially actions undertaken to adapt the initial certification process, start ex officio oversight and enforcement actions**, as well as the efforts made by the U.S Government by publishing a number of important documents and **the appointment of a new Chair as well as of two new members of the PCLOB, meaning that the PCLOB has reached the required quorum for its functioning**. However, **the EDPB still has a number of significant concerns that need to be addressed by both the Commission and the U.S. authorities**.

26. **The absence of substantial checks remains a concern of the EDPB. Other areas that require further attention are the application of the Privacy Shield requirements regarding onward transfers, HR Data and processors, as well as the recertification process**. In addition, the EDPB recalls the **remaining issues** with respect to certain elements of the commercial part of the Privacy Shield adequacy decision as already raised in the WP 29's Opinion 01/2016.

27. As regards the **collection of data by public authorities, the EDPB can only encourage the PCLOB to issue further reports**, including on PPD-28 to follow up on the first report in order to provide additional elements as to how the safeguards of PPD-28 are applied, on Section 702 FISA, and Executive Order 12333.

28. **On the Ombudsperson mechanism**, the EDPB is **still awaiting the appointment of a permanent independent Ombudsperson**. Given the elements provided, **the EDPB is not in a position to conclude that the Ombudsperson is vested with sufficient powers to access information and to remedy non-compliance, and it can thus not state that the Ombudsperson can be considered an "effective remedy before a tribunal" in the meaning of Art. 47 of the EU Charter of Fundamental Rights**.

29. Finally, the EDPB recalls that the **same concerns will be addressed by the European Court of Justice in cases that are already pending** before the Court.

2 INTRODUCTION

30. On 6 October 2015[3], the European Court of Justice invalidated the Safe Harbor adequacy decision after having recalled the important role played by the protection of personal data in the light of the fundamental right to respect for private life and the large number of persons whose fundamental rights are liable to be infringed where personal data is transferred to a third country not ensuring an adequate level of protection. Soon after, the Commission started negotiations for a new adequacy decision and presented a draft adequacy decision with its annexes.

31. On the 13 April 2016, the Working Party 29 issued an opinion[4] on the draft new adequacy decision aiming at replacing the invalidated Safe Harbor. On the same day, the WP29 also issued a working document[5] on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees).

32. On 30 May 2016, the European Data Protection Supervisor also issued an Opinion on the draft adequacy decision[6].

33. On 12 July 2016, the European Commission adopted the EU-U.S. Privacy Shield adequacy decision[7] ("Privacy Shield"). The Privacy Shield entrusts the Commission with the task to assess the findings of the adequacy decision, including on the basis of the factual information collected in the context of an Annual Joint Review[8]. Important concerns on both the commercial aspects and aspects relating to government access to personal data transferred under the Privacy Shield for the purposes of Law Enforcement and National Security had then to be addressed and further assessed in the context of the Joint Review.

34. As also foreseen in recital 147, *"participation in this meeting will be open for EU DPAs and representatives of the Article 29 Working Party"*.

35. The WP 29 also issued a report following the first Joint Review of the Privacy Shield in November 2017[9].

36. The second Joint Review of the Privacy Shield took place on the 18 and 19 October 2018 in Brussels. In addition to the Chair of the EDPB who gave an introductory speech, seven representatives of the EDPB, a Commissioner as well as experts at staff level, were designated to be part of the Review Team ("the Review Team") that accompanied the Commission during this two-day meeting with U.S. authorities and companies.

[3] Case C-362/14
[4] WP 238 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf
[5] WP 237 https: //ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp237_en.pdf
[6] EDPS Opinion 4/2016 of 30 May 2016: https://edps.europa.eu/sites/edp/files/publication/16-05-30_privacy_shield_en.pdf
[7] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, OJ L 207, 1.8.2016, p.1.
[8] See recitals 145-149 and Article 4(4) of the decision.
[9] WP 255: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48782

37. In advance to the Joint Review, the Commission sent questionnaires to US companies adhering to the Privacy Shield and NGOs, as well as a detailed agenda to organize the discussions with the US authorities and stakeholders during the Joint Review itself. The EDPB sent contributions to take part to the elaboration of these documents.

38. The new factual elements presented by the US authorities and companies participating in the Joint Review, stemming both from written submissions, as well as from oral contributions during the Joint Review itself, are presented in annex to this document. They were presented at the EDPB Plenary on 16 November.

3 ON THE COMMERCIAL ASPECTS OF THE PRIVACY SHIELD

3.1 Guidance for the companies adhering to the Privacy Shield

39. The EU-U.S. Privacy Shield is an adequacy decision that was designed to frame transfers of personal data outside the protections provided under GDPR to ensure the level of protection of natural persons guaranteed by GDPR is not undermined in the absence of a general law in the US providing for an essentially equivalent level of protection of personal data. It is of utmost importance that there is a common understanding of the text to ensure the application in the receiving State will correspond to the requirements for such transfers as set out under EU data protection law. It has to be ensured that this text is interpreted correctly and that organizations and individuals on both sides of the Atlantic are "on the same page" as regards their duties and rights under the Privacy Shield.

40. Thus, in the report of the first annual review the WP 29 emphasized the need for clear guidance on the application of the Privacy Shield principles. In the second year of operation of the framework and following informal consultation of members of the ITS at working level, the DoC has issued **guidance in the form of FAQs on the Accountability for Onward Transfer Principle**[10] **and the notion of Processor**[11] and published it on its website.

41. The EDPB welcomes the issuance of these guiding documents that have been also highly demanded by participating organizations. This guidance should lead to the clarifications necessary to facilitate the proper application of the Privacy Shield Principles. In order to achieve this goal, the guidance concerning processors may further specify the application of the principles when it comes to processors ("agents")[12].

42. Regarding the usability of the European Commission's Standard contractual clauses in the context of onward transfers further work is required since the available clauses are designed only for transfers from EU territory. In this context the EDPB calls upon the European Commission to also address this issue in the course of aligning the SCC with GDPR.

43. The EDPB regards the issuance of further guidance as a good start and expects that in the future there will be more guidance as to other key elements such as for example the **Choice Principle**, (on when and how a data subject can opt out from the processing of his/her data for a new purpose), and with respect to the **application of the Notice Principle** (more specifically on the timing for certified organizations to give notice to individuals). In addition, a **clarification of the scope of the right of access** could be helpful to prevent misunderstandings. In its last report worries regarding the possibly very narrowly interpreted duty to grant the right of access only to data that is "stored" by an organization voiced by the WP 29 remains valid.

3.2 Clear and easily available information for EU individuals

44. The WP 29 had found that to complement the specific information provided in concrete cases by the companies themselves, the US authorities should strive to offer **more information in an accessible and easily understandable form to the individuals regarding their rights and available recourses and remedies.**

45. The Privacy Shield website already had a specific section named "EU and Swiss individuals" containing subsections "My rights under Privacy Shield" and "Privacy Shield participants list"[13] where individuals were informed about their rights. The various possibilities to lodge complaints were also explained and partly supported by direct links. After the first annual review and as a response to the WP 29s suggestions the DoC added a one-page document to their website that gives individuals an overview[14] of the program with a strong focus on the individual's rights and how they can be exercised. The EDPB acknowledges the efforts made by the DoC to provide further guidance for EU individuals on the Privacy Shield website. It remains to be seen if the Information given to the EU individuals both by the EU Supervisory Authorities and the DoC lead to the effect that more individuals are able to exercise their rights regarding the Privacy Shield properly.

3.3 Self-(Re)Certification Process and Cooperation between U.S. authorities in the Privacy Shield mechanism

46. Also in the certification process, the EDPB notes improvements:

47. The DoC reviews all self-certifications (both for first time applicants and for recertification submissions) and checks:

    1. Registration with an Independent recourse mechanism (IRM) company
    2. Payment of Annex I Arbitral Fund Contribution
    3. Compliance with Privacy Shield supplemental principle 6 (on access to personal information)
    4. Completion and consistency of certification information

[10] https://www.privacyshield.gov/article?id=Onward-Transfer-Principle-FAQs (last accessed on 18 December 2018)
[11] https://www.privacyshield.gov/article?id=Processing-FAQs (last accessed on 18 December 2018)
[12] that the guidance could for example further elaborate on the following details: Notice to be provided by processors needs to be in line with the contract in place between the processor and the controller; that access to data and a Choice mechanism could be provided to the individual directly by the processor provided however that the controller has in the first place authorized the processor to do so; and that for a processor compliance with the Data Integrity and Purpose Limitation principle requires it to process the data only in accordance with the instructions from the controller and on the other hand to implement the appropriate measures as instructed by the controller to assist the later in complying with the data integrity principle.

[13] See: https://www.privacyshield.gov/Individuals-in-Europe (last accessed on 27 November 2018)
[14] See: https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000000QJdq (last accessed on 14 December 2018)

5. Privacy notices (the existence of all 13 elements required by the Privacy Shield is checked also in the organizations Privacy Policy)

48. In order to prevent organizations from naming non-U.S subsidiaries as entities covered by their certification the DoC has produced more internal guidance for the review of applications regarding the identification of foreign entities.

49. Also, the DoC asks the organizations for more precise links provided for the Privacy Shield listing so individuals can more easily exercise their rights and for more than one point of contact within the organization to make sure messages from the DoC are received. The DoC also checks the applications for inconsistencies between the privacy policy and the certification (For example HR/NON HR).

50. The DoC has not finalized 100 first-time certifications and 30 re-certifications because the requirements set out by the Privacy Shield were not fulfilled. This appears to be an indication that the decision made by the DoC whether or not to list an organization on the Privacy Shield website is – as far as the checks go - not a rubber stamp exercise.

51. However, on the basis of the information given by the US authorities during the joint review, so far those checks do not go into the substance of the principles. The DoC for example does not check if the data transferred to an organization in the US acting as a controller is necessary and proportionate to the purpose, arguing that the Privacy Shield does not provide for checks with this level of detail. This absence of substantial checks remains a concern for the EDPB on the general question of sufficient oversight regarding the substance of the Privacy Shield principles.

52. As regards criticism on the procedure, which used to require US organizations to publish their Privacy Policy (with references to the Privacy Shield) before the checks of the DoC were finalized and the organization was put on the list of Privacy Shield active participants, the DoC has changed its procedure. The Doc now prohibits a first-time applicant from making public representations about participation until the PS Team approves its certification and instead requires an applicant to submit a draft privacy policy for review. It also directs an applicant to remove any premature references of their participation in the Privacy Shield program from their website.

53. As a result, **the concerns of the WP 29 regarding the inconsistencies between the Privacy Shield List and the representations made by the organizations on their websites seem to have now been resolved as far as the initial certification process is concerned**.

54. **Regarding the re-certification process**, the second annual review revealed that due to the established procedures there are cases where the due date displayed on the Privacy Shield List is already passed while the organization still is listed as an active participant. This occurs when an organization has submitted their recertification but the process is not finalized before the due date. This leads to confusion.

55. As long as the organizations still publicly commit to apply the Privacy Shield Principles this might not lead to a gap in the protection of individuals. **However the EDPB asks the DoC to explore what can be done to avoid this situation** (especially what can be done to guarantee that there is no gap in the protection of individuals) **and in the meantime to add some explanation for concerned individuals and EU based organizations using the Privacy Shield as a transfer tool so the situation is sufficiently clear to individuals and also organizations within the EU that would like to transfer personal data to a Privacy Shield certified organization and therefore check the validity of the certification on the Privacy Shield List**.

3.4 Oversight and supervision of compliance with the Principles – Activities of the DoC

56. In last year's report the WP 29 criticized that the **oversight of the commercial aspects of the Privacy shield mainly relied on the third party companies providing Independent Recourse Mechanisms (IRMs)** and that the **implementation** of the Privacy Shield framework **lacked sufficient oversight and supervision of compliance in practice**. Because the Privacy Shield is a program based on self-certification, it is of utmost importance that U.S. authorities involved in the administration of the Privacy Shield devote sufficient resources at oversight and enforcement activities. The WP 29 considered that the **performance of compliance reviews** of organizations having self-certified to the Privacy Shield is a key element for the effective functioning of the framework and that **ex-officio investigations have to be conducted both by the DoC and the FTC/DoT** to ensure that self-certified organizations concretely implement the requirements of the Privacy Shield.

57. This year's review showed that the U.S. authorities (namely DoC and FTC) have made significant efforts to address this concern:

- On a quarterly basis the DoC conducts "false claims reviews" in order to identify organizations that have started but not finished an initial or re-certification or that did not submit their annual re-certification at all.
- The identified organizations receive a certified letter from the DoC, warning them of potential referrals to the FTC or DoT if they do not fulfil outstanding requirements or withdraw properly from the program. The DoC informs the FTC/DoT of its intent to send those letters. The organizations have 30 days to respond to the letter. The DoC compiles a list of those organizations that fail to take action and respond to the letter. This procedure has led to 100 referrals from the DoC to the FTC, 56 of those referral were made in the second year of the Privacy Shield program. DoC and FTC/DoT cooperate throughout the whole process. Simultaneously with the referral an organization is (at least temporarily) removed from the "active" Privacy Shield List.
- As foreseen in the Privacy Shield text, the DoC also performs random web searches for false claims of participation in the program. Those web-searches have only led to few cases that were referred to the FTC.
- The DoC has performed a sweep of 100 randomly chosen organizations. The focus of the sweep was the accessibility of the Privacy Policy, the responsiveness of the organization and the availability of the IRM. The DoC sent more in-depth compliance questionnaires to 21 organizations that showed minor or more significant peculiarities (for example: No response from the designated point of contact; the Privacy policy was no longer accessible online; Missing references to one or more elements of the notice principle). The organizations must respond within 30 days. If the response is not satisfactory, the organizations – similar to the procedure described above – receive a certified warning letter requiring the organization to indicate within a 30 day period how it has addressed the concerns. If those are not resolved within the 30 days the organization is moved to the "inactive" list and the case is being referred to the FTC or DoT.
- The DoC has also designated 1 person to follow the media and to do keyword searches to identify possible breaches of the Privacy Shield commitments.

- The DoC also performs regular checks for broken links to the privacy policy on the Privacy Shield list.

58. **The EDPB welcomes all these steps taken by the DoC to ensure formal compliance with the Principles of the Privacy Shield. They are a good starting point; however, so far these checks remain focused on the formalities to be complied rather than on the substance.**

59. Further to monitoring concrete compliance with all principles of the framework, one of the areas that would need particular attention in this context remains the area of onward transfers. So far the DoC has not made use of its right to request a copy of the relevant privacy provisions of organizations contracts with their agents. Since onward transfers possibly lead to transfers of data outside of the jurisdiction of U.S. and EU authorities with possibly no data protection provided by law it is of utmost importance to closely monitor the practical implementation of the Accountability for the Onward Transfers Principle.

3.5 Oversight and supervision of compliance with the Principles – Activities of the FTC

60. Since last year's review the FTC also increased their activities regarding the enforcement of the Privacy Shield.

61. In the Division of Privacy and Identity Protection, Bureau of Consumer Protection there are 40 lawyers almost exclusively working only on privacy. They are supported by for example technical experts.

62. This year the FTC has brought 5 new Privacy Shield cases: 2 against organizations that did not complete their certification and 3 cases where the certification has lapsed. In most of those cases, the organization failed to verify the deletion, return or continued application of the Privacy Shield Principles to personal data transferred under the Privacy Shield.

63. The FTC investigates Privacy Shield-related referrals (about around 100 referrals, 8 of them being public) but in most cases by the time these referrals arrive to the FTC they have been solved in the meantime so many cases fall out.

64. As an experiment, the FTC has started to send out Civil Investigation Demands (CIDs) proactively to monitor compliance with the Privacy Shield Principles. The FTC could not provide more details on the selected targets or topics of this exercise. In general the FTC has a broad latitude to do sweeps. There is no need for the FTC to demonstrate that it has a reasonable suspicion. The objective is rather to identify where it is profitable to spend the resources.

65. **The EDPB welcomes the ex officio activity to proactively monitor compliance with the Privacy Shield Principles undertaken by the FTC. It nevertheless regrets that the FTC was unable to share any more detail on its approach as this leaves the EDPB unable to have a clear insight on the concrete activities and cases, and therefore to be in a position to assess how and to what extent the FTC ensures compliance monitoring with the substance of the Privacy Shield's principles.**

3.6 Independent Recourse Mechanisms

66. In order to make the reports provided by the various companies providing IRM services on an annual basis more useful the DoC gave out guidance to the IRM services in order to harmonize their reports. This guidance also highlights the possible conflicts of interest within companies providing both ex officio compliance and IRM services to the same organization and asks to describe the measures taken

to avoid such conflict of interests in the annual report. **The EDPB expects to see improved and comparable reports provided by the IRM services in the next annual review, that also explain how possible conflicts of interests are precluded.**

3.7 HR Data

67. As already stated by the WP 29 in last year's report, the notion of HR data in the context of the Privacy Shield is interpreted differently within the EU and by the US authorities. Although the DoC initiated the producing of guidance regarding the processing of HR data, including through informal consultation of members of the WP 29 on working level in this regard, the work on this guidance was not successful due to the absence of convergence on the definition of the notion of HR data. This year's review thus focused less on the definition of HR data but rather on the consequences, the different definitions within the EU and by US authorities may lead to. On the EU side, the concern is that additional protections granted by the Privacy Shield for employment data (opt-in to marketing purposes rather than opt out) would not and could not be enforced by any U.S or EU authority. The EDPB recalls that in its understanding, HR data should be protected in the same way whether they are processed by the employer or by a processor, including concerning the choice and purpose limitation principles. While the EU Supervisory authorities remain available to exchange with the US Authorities, the discussions on this issue will have to continue between the European Commission and the US Authorities given the different possible readings of the wording of the Privacy Shield. **In parallel, the Commission is still called upon to address this issue and clarify the text in order to avoid that possible different interpretations do not lead to gaps in the protection of employees in the European Union.**

3.8 Automated-decision making/Profiling

68. In last year's report, the WP29 **called upon the Commission to contemplate the possibility to provide for specific rules concerning automated decision making** to provide sufficient safeguards including the right to know the logic involved and to request reconsideration on a non-automated basis, especially after having explored the extent of the practical relevance of automated decision making processes by Privacy Shield certified companies if the analysis generates an actual need for additional safeguards.

69. As part of the second review the COM presented the main elements of a study[15] commissioned to an independent contractor regarding the existence of automated decision-making on the basis of personal data that has been transferred from the EU to Privacy Shield certified companies in the US. While the authors of the study highlight a series of challenges for conducting this work (limited availability of experts on the topic and reservations to take part in interviews, limited relevance of answers in certain cases, opacity characterizing the data industry on such practices notably), the main conclusion that can be drawn from the study is that **automated decisions (in the narrow GDPR definition of decisions having legal effects on individuals) are not taken on the basis of data transferred from the EU.**

70. According to the study, such decisions are more likely to take place in "EU customer facing" situations (i.e. where the US company directly targets EU customers).

[15] See: https://ec.europa.eu/info/sites/info/files/independent_study_on_automated_decision-making.pdf (last accessed on 19 December 2018)

71. **However, the study at the same time underlines that this is a fast developing area which still has to be closely monitored in the future.**

72. Some private companies (such as Workday and Salesforce) confirmed that they are offering services to their customers (EU businesses) which can be AI-based and potentially conduct some automated decisions[16]. However, these companies insisted that in any case they always act as data processors under the instructions of data controllers based in the EU.

73. According to the study, several credit-reporting agencies have self-certified under Privacy Shield (notably Experian, one of the three big major reporting companies in the US). The FTC has general enforcement jurisdiction over these agencies, in cooperation with the US Consumer financial bureau, which has supervisory authority over credit-reporting agencies (such companies have different products - some of these products may fall under the US Fair Credit Reporting Act). The Consumer financial bureau would pass on cases to the FTC so the same principles apply to such companies and if they are misrepresented the FTC would enforce them.

74. The FTC publicly announced that they are investigating the Equifax data breach case[17].

75. The FTC also presented the RealPage company case[18], which is offering background screening services by conducting criminal checks and automated decisions making by using weak accuracy verification methods[19]. The FTC asked the company to put in place a better, reasonable procedure to ensure first names' accuracy. This case led to a 3 million dollars fine settlement[20].

76. There was no other significant new developments as regards Automated Decision Making to take note of.

77. **The EDPB invites the European Commission to monitor cases related to automated decision making and profiling and to contemplate the possibility to foresee specific rules concerning automated decision making to provide sufficient safeguards, including the right to know the logic involved and to request reconsideration on a non-automated basis where an actual need for additional safeguards is identified.**

[16] See for example the "Prism Analytics" tool offered by Workday which allows companies to "bring data in at scale from any source and prepare, analyze and securely share it with[in the] organization" (see https://www.workday.com/en-us/applications/prism-analytics.html) and the AI-based predictive marketing tool "Einstein" proposed by Salesforce (see: https://www.salesforce.com/products/einstein/overview/).
[17] See: https://www.ftc.gov/equifax-data-breach (last accessed on 28 November 2018).
[18] See: https://www.ftc.gov/news-events/press-releases/2018/10/texas-company-will-pay-3-million-settle-ftc-charges-it-failed (last accessed on 28 November 2018).
[19] According to the abovementioned US FTC's press release: *"(...) RealPage compiled screening reports through an automated system that used the applicant's first name, middle name when available, last name, and date of birth when searching for criminal records. Its matching criteria only required an exact match of an applicant's last name along with a non-exact match of a first name, middle name, or date of birth, the FTC alleges. For example, if RealPage searched an applicant named Anthony Jones born on October 15, 1967, it would deem a match if it found a criminal record for Antony Jones 10/15/67, Antonio Jones 10/15/67 and Antoinette Jones 10/15/67."*
[20] See: https://www.ftc.gov/enforcement/cases-proceedings/152-3059/realpage-inc

4 ON THE DEROGATIONS TO THE PRIVACY SHIELD TO ALLOW ACCESS TO DATA FOR LAW ENFORCEMENT AND NATIONAL SECURITY PURPOSES

4.1 Introduction

78. **The EDPB welcomes that the U.S. government has continued to publish a number of important documents**, e.g. decisions by the Foreign Intelligence Surveillance Court[21] (FISA Court), in part by declassification, as well as through the new website set up. These publications and declassifications continue to demonstrate the efforts by the U.S. government and of the U.S. legislator to become more **transparent** about the use of surveillance powers. In addition, these documents help to better understand how the various surveillance programs are operated, including their safeguards. The additional explanations and answers provided during the two Joint Reviews also helped the EDPB to get a clearer understanding of these programs and safeguards and of their concrete impact on the level of data protection in place.

79. Nevertheless, some of the main points of concern that the WP29 expressed in its previous opinions, in the area of access to data transferred under the Privacy Shield for national security or law enforcement purposes, have not been fully resolved. These **main concerns are related to the collection of data, to oversight, to judicial redress and finally, to the Ombudsperson mechanism. This calls for a more detailed analysis.**

4.2 Collection of data (under section 702 and under EO 12333)

4.2.1 Collection of data for national security purposes under Section 702

80. In its Schrems judgment[22], the CJEU recalled that the *"protection of the fundamental right to respect for private life at EU level requires derogations and limitations in relation to the protection of personal data to apply only in so far as is strictly necessary"*[23] and ruled that *"legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter"*[24].

81. **The previous concerns expressed by the WP29 remain relevant, as** the legal framework has not significantly changed on any of the aspects concerning the collection of data from the perspective of EU individuals. Therefore the EDPB recalls the concerns expressed previously by the WP29 in this respect.

82. The **EDPB also regrets that in the context of the re-authorization of section 702 FISA last year, the US legislator did not take the opportunity to introduce additional safeguards**.

83. The EDPB thus maintains its call for further independent assessment on the necessity and proportionality of the definition of "targets" and of the tasking of selectors under section 702 (including in the context of the UPSTREAM program), as well as the concrete process of application of

[21] U.S. federal court established and authorized under the Foreign Intelligence Surveillance Act of 1978 (FISA)
[22] Case C-362/14, 5 October 2015
[23] See recital 92, See also cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger, recital 52.
[24] See recital 94.

selectors in the context of the UPSTREAM program to clarify whether massive and indiscriminate access to personal data of non-U.S. persons takes place.

84. **The EDPB would welcome if the Privacy and Civil Liberties Oversight Board (PCLOB), as an independent oversight agency with a quorum (see infra), should now be in a position to prepare and issue an updated report on Section 702, building on the report issued in 2014.**

4.2.2 Collection of data for national security purposes under Executive Order 12333

85. **In the context of the second Joint Review, given the disagreements between the EDPB, on the one hand, and the European Commission and the US authorities on the other, as to the relevance of Executive Order 12333 for the adequacy decision, the application of legislation was not further discussed.**

86. The EDPB recalls the WP29 long-standing position that the analysis of the laws of the third-country for which adequacy is considered, should not be limited to the law and practice allowing for surveillance within that country's physical borders, but should also include an analysis of the legal grounds in that third country's law which allow it to conduct surveillance outside its territory as far as EU data are concerned. Necessary limitations to governmental access to data should extend to personal **data "on its way" to the country, for which adequacy is recognized**. This is why the WP29 analysed the Executive Order 12333 and the Presidential Policy Directive 28 (PPD-28), which is all the more important in this context as it provides for the only safeguards and limits to the collection and use of data collected outside the U.S. as the limitations of FISA or other more specific U.S. law do not apply. During the Joint Review, the U.S. authorities underlined again that Executive Order 12333 could not be used as a basis for collection of data inside the U.S. territory and that they consider that collection of data under this Executive Order falls outside the scope of the Privacy Shield.

87. The WP29 welcomed the adoption of PPD-28. The current U.S. government confirmed its commitment during the Joint Review to comply with the rules set therein, which the EDPB welcomes. Indeed, the PPD-28 provides limitations to the collection of data, as the signal intelligence activities have to be as "tailored as feasible". The EDPB notes that the recently published report by the PCLOB on PPD-28 confirms that it has been transposed into the internal policies of the relevant authorities. **However, neither the report nor the Second Joint Review provided substantial new information concerning the application of this text,** especially on the interpretation of the six purposes allowing for the use of data foreseen in this text, or on additional elements as to the amount of personal data collected in order to allow for a validation of the commitments and the assurances provided. Here again, given the uncertainty and unforeseeability of how EO 12333 is applied, the EDPB would welcome if the PCLOB finished and issued its awaited report on EO 12333 to provide information on the concrete operation of this Executive order and on its necessity and proportionality.

88. In addition, a more detailed follow-up report on how the PPD-28 applies to the different surveillance programs would be welcome to provide additional elements on these aspects.

4.3 Oversight

89. The EDPB recalls that comprehensive **oversight of all surveillance programs** is crucial, as the CJEU and the ECtHR have also emphasized in many judgments.

90. **Additional presentations were made during the second Joint Review by the different institutions of which the oversight structure consists. Although these elements brought few new elements, they confirmed the understanding of the EDPB, of the architecture and functioning of the Inspector General community.**

91. Already during the first annual Joint Review, the WP29 was presented with the oversight activities of several entities and considers that a **comprehensive internal oversight structure**, independent from the Intelligence Community, is in place, including the Privacy and Civil Liberty officers, the oversight of the Department of Justice, and Inspector Generals, amongst others.

92. As expressed in the previous opinions of WP29, the EDPB is aware of the complex and multi-layered oversight structure established in the U.S. in order to ensure that personal data is collected and processed in accordance with U.S. law. As underlined in the previous report of the WP29, the EDPB remains of the view that the offices of **the Inspector Generals**, institutions rarely known in most EU Member States, provide valuable checks on the US government's agencies.

93. **The EDPB welcomes the appointment of a new Chair as well as of two new members of the PCLOB. This means that the PCLOB has reached the required quorum for its functioning just before the second Joint Review, although the remaining vacant positions and the requirement for this organ to be bipartisan are yet to be fulfilled.** As emphasized before, the EDPB considers the **PCLOB,** whose recommendations have been an important contribution to reforms in the U.S. and whose reports have been a particularly helpful source to understand the functioning of the various programs, as an independent body, to be an essential element of the oversight structure.

4.4 Redress for EU individuals

94. In its Schrems ruling, the CJEU stressed the importance to have a right to an effective remedy before a tribunal[25]. A third-country can only be considered as providing an adequate level of protection in accordance with the GDPR, where EU individuals have access to an independent and impartial redress body, including in surveillance matters.

95. **As the U.S. government informed during this year's Joint Review that the legal framework remained unchanged and no significant new case law concerning these matters needed to be considered, the EDPB recalls its position and the relevant criteria to take into account when assessing the level of adequacy are still those stemming from the jurisprudence of the highest courts in Europe, meaning the CJEU and ECtHR**.

96. As underlined in the previous report of the WP29, while the APA and FISA appear to provide limited grounds for an EU individual to challenge surveillance in U.S. courts, the principal problem appears to concern the **"standing requirement"**.

97. Under the procedural requirements as currently interpreted by the U.S. courts, it appears to be difficult and uncertain that an EU individual could satisfy the procedural requirement of standing when bringing a suit against a surveillance measure on the basis of section 702 FISA or EO 12333. The EDPB will therefore continue to follow closely the evolution of these cases as they could provide additional guarantees concerning the effectiveness of judicial redress offered before U.S. courts. However, as was confirmed during the Joint Review, the interpretation of the notion of "standing" in surveillance matters is evolving with cases still pending[26].

[25] See paragraph 95
[26] See in particular cases ACLU v. Clapper, and Wikimedia v. NSA

4.5 Ombudsperson mechanism

98. **The most significant element in the context of the second Joint Review was the nomination of a new acting Ombudsperson, Mrs Manisha Singh, on 28 September 2018.**

99. Since the effective remedy before an independent tribunal is of such importance in the jurisprudence of the European courts, the WP29 welcomed the establishment of an **Ombudsperson** mechanism as a new redress mechanism in its previous opinion. It underlined that this may constitute a significant improvement for EU individuals' rights with regards to U.S. intelligence activities. The Ombudsperson mechanism complements the possibilities of redress, or more critically, it might be argued that it is meant to compensate for the uncertainty or unlikeliness to seek effective redress before a U.S. court in surveillance matters. In addition, as the PPD-28 does not create rights, it was confirmed that the individual cannot go to court based on an alleged violation of the PPD-28. Thus, the only way for EU individuals to ask for a verification that the relevant authorities have complied with the requirements of this instrument is to ask the Ombudsperson to refer the matter to the competent Inspector General to check the internal policies of these authorities.

100. With Art. 47 of the Charter of Fundamental Rights in mind, the threshold for independence and impartiality required in a redress mechanism such as the Ombudsperson is high. Having analysed the jurisprudence of the ECtHR in particular, the WP29 took into account the powers of the Ombudsperson, in particular the powers to access information as well as to remedy non-compliance. When assessing the Ombudsperson mechanism in its opinion and its report of last year, the WP29 suggested that the appointment of a high-ranking official in the Department of State as the Ombudsperson, who can be dismissed at any time without notice, is problematic.

101. During the first and the second Joint Review, as well as before the EDPB Plenary in July 2018, the previous and new acting Ombudspersons and the U.S. government explained in some detail the important work done in order to ensure that requests would be handled lawfully and efficiently. The two acting Ombudspersons also stressed that they needed to be convinced of the findings before responding to the request and Mrs Singh also underlined during the second Joint Review that she could escalade the issue should she be unconvinced by the outcome presented to her following the assessment of a request. While the EDPB still has no reason whatsoever to doubt the integrity of the new (acting) Ombudsperson, **it recalls that a permanent Ombudsperson should be appointed as soon as possible as well as its expectation to learn more about the powers that the Ombudsperson has vis-à-vis the Intelligence Community**. This information however remains partial. The procedures governing the access to relevant information by the Ombudsperson and governing the interactions of the Ombudsperson with the other members of the Intelligence Community, including the oversight bodies, remain partially classified. The EDPB acknowledges that the acting Ombudsperson explained how a theoretical case would be handled during the Joint Review.

102. Based on the available information, the EDPB still doubts that the powers to remedy non-compliance vis-à-vis the intelligence authorities are sufficient, as the "power" of the Ombudsperson seems to be limited to decide not to confirm compliance towards the petitioner. In the understanding of the EDPB, the (acting) Ombudsperson is not vested with powers, which courts or other similarly independent bodies would usually be granted to fulfil their role. Therefore, the EDPB remains unable to hold that the Ombudsperson is vested with adequate powers to effectively exercise its duty. In addition, it was confirmed during the Joint Review that the decisions of the Ombudsperson cannot be brought to court.

103. The EDPB recalls the lack of judicial review of the decisions of the Ombudsperson and consequently the impossibility to obtain remedies where the Ombudsperson will not provide any answer. **As a conclusion, the EDPB is not be in a position to conclude that the Ombudsperson is vested with sufficient powers to access information and to remedy non-compliance, and it can thus not state that the Ombudsperson can be considered an "effective remedy before a tribunal" in the meaning of Art. 47 of the Charter of Fundamental Rights.**[27]

4.6 Access to data for law enforcement purposes

104. As regards **access to data for law enforcement purposes**, the EDPB continues to note that the procedural safeguards inherent to the criminal procedure seem to imply that data are accessed for a specific purpose and that individuals are notified that their data have been accessed within the framework of criminal proceedings, in the context of which they can have access to judicial redress. However, it recalls its concerns as regards effective remedies available to individuals in cases where the data processed by companies is accessed by law enforcement authorities, as underlined in the previous opinion issued by the WP29[28].

5 CONCLUSION

105. The EDPB **welcomes the efforts made by the U.S. authorities and the Commission to implement the Privacy Shield, especially actions undertaken to adapt the initial certification process, start ex officio oversight and enforcement actions,** as well as the efforts made by the U.S Government by publishing a number of important documents **and the appointment of a new Chair as well as of two new members of the PCLOB, meaning that the PCLOB has reached the required quorum for its functioning.**

106. However, **the EDPB still has a number of significant concerns that need to be addressed by both the Commission and the U.S. authorities**.

107. **The absence of substantial checks remains a concern of the EDPB. Other areas that require further attention are the application of the Privacy Shield requirements regarding onward transfers, HR Data and processors, as well as the recertification process.** In addition, the EDPB recalls the **remaining issues** with respect to certain elements of the commercial part of the Privacy Shield adequacy decision as already raised in the WP 29's Opinion 01/2016.

108. As regards the **collection of data by public authorities**, **the EDPB can only encourage the PCLOB to issue further reports**, including on PPD-28 to follow up on the first report in order to provide additional elements as to how the safeguards of PPD-28 are applied, on Section 702 FISA, and Executive Order 12333.

109. **On the Ombudsperson mechanism**, the EDPB is **still awaiting the appointment of a permanent independent Ombudsperson**. Given the elements provided, **the EDPB is not in a position to conclude that the Ombudsperson is vested with sufficient powers to access information and to remedy non-compliance, and it can thus not state that the Ombudsperson can be considered an "effective remedy before a tribunal" in the meaning of Art. 47 of the EU Charter of Fundamental Rights**.

[27] A first request from an EU individual was received under the Ombudsperson mechanism at the end of 2018.
[28] WP 238

110. Finally, the EDPB recalls that the **same concerns will be addressed by the European Court of Justice in cases that are already pending** before the Court.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

ANNEX TO THE EDPB REPORT ON THE SECOND EU-US PRIVACY SHIELD ANNUAL JOINT REVIEW

Factual findings of the second annual joint review of the EU-US Privacy Shield

GENERAL INFORMATION

1. The U.S. Delegation was composed of high level representatives.
2. As of now, the Privacy Shield List contains around 3944 organizations, 338 are on the "Inactive" List either because they have withdrawn from the program (38), not recertified or because their certification has lapsed. There was no case where an organization was removed from the List because it persistently failed to comply.
3. GDPR has led to an increase of interest in the Privacy Shield. The DoC has about 1000 more certifications under review.
4. The DoC has increased their staff to 12 persons now that exclusively work on the Privacy Shield.

1 ON COMMERCIAL ASPECTS

1.1 Self-Certification Process and Cooperation between U.S. authorities in the Privacy Shield Program

5. The DoC reviews all self-certifications (first time applicants as well as recertification submissions) for:
    1. Registration with IRM
    2. Payment of Annex I Arbitral Fund Contribution
    3. Compliance with supplemental principle 6
    4. Completion and consistency of certification information
    5. Privacy notices
6. DoC has not finalized 100 first-time certifications and 30 re-certifications because the requirements set out by the Privacy Shield were not fulfilled.
7. As regards the depth of the analysis the DoC performs: the DoC checks the applications for inconsistencies between the privacy policy and the certification (For example HR/NON HR). It does not check if the data transferred is necessary and proportionate to the purpose because they consider that the Privacy Shield does not go into this level of detail.
8. In order to address the concern expressed by the WP29 regarding the duty of the certifying organization to publish their privacy policy referring to the Privacy Shield certification before the DoC has completed the exercise of checking and listing the organization, the DoC has changed the procedure.
9. The DoC now:
    - Prohibits a first-time applicant from making public representations about participation until the PS Team approves its certification
    - Requires an applicant to submit a draft privacy policy for review

- Directs an applicant to remove any premature references

10. As the practical experience with the certification process increases the DoC has refined their procedures and now for example have produced more guidance for the review of applications regarding the identification of foreign entities; they ask the companies for more precise links so individuals could more easily exercise their rights, they ask for more than one point of contact within the organization to make sure messages from the DoC are received.

11. 2 weeks before a certification reaches its next certification due date, the DoC sends the organization a notice to remind them of the need to re-certify if the organization wishes to stay on the "active" List.

12. The organizations that want to stay in the Privacy Shield program are obliged to communicate their re-certification by the due date.

13. However, the re-certification process is usually not finished by the due date which leads to organizations being listed as "active" while the due date for re-certification has "expired". A very common reason for this is for example an unpaid fee. The DoC then has to go back to the organization to explain what needs to be done.

14. The DoC emphasized that even if the due date for re-certification on the Privacy Shield list is in the past, there is no gap in the protection because the protection is provided by the public commitments made by the organizations.

15. However they agreed that this situation might be confusing for companies or individuals checking the listing of an organization and seemed to agree that it would at a minimum be helpful if the Privacy Shield website itself would provide an explanation on why an organization is still on the "active" list while the due date for the re-certification has expired.

16. Once the organization has submitted its application for re-certification it is required to complete its certification within 45 days. If it fails to meet this deadline, it is required to remove any references to its participation in the Privacy Shield Program and it might face referral to the FTC.

1.2 Oversight and supervision of compliance with the principles - Activities by the DoC

17. On a quarterly basis the DoC identifies organizations that have started but not finished an initial or re-certification or that did not submit their annual re-certification at all.

18. The identified organizations receive a certified letter from the DoC, warning them of potential referrals to the FTC or DoT if they do not fulfil outstanding requirements or to withdraw properly from the program. The DoC informs the FTC/DoT of its intent to send those letters. The organizations have 30 days to respond to the letter. The DoC compiles a list of those organizations that fail to take action and respond to the letter. This procedure has led to 100 referrals from the DoC to the FTC, 56 of those referral were made in the second year of the Privacy Shield program. DoC and FTC/DoT cooperate throughout the whole process. Simultaneously with the referral an organization is (at least temporarily) removed from the "active" Privacy Shield List.

19. As foreseen in the Privacy Shield text, the DoC also performs random web searches for false claims of participation in the program. Those web-searches have only led to few cases that were referred to the FTC.

20. The DoC has performed a sweep of 100 randomly chosen organizations. The focus of the sweep was the accessibility of the Privacy Policy, the responsiveness of the organization and the availability of the IRM. The DoC sent more in-depth compliance questionnaires to 21 organizations that showed minor or more significant peculiarities (for example: No response from designated point of contact; Privacy policy was no longer accessible online; Missing references to one or more elements of the notice principle). The organizations must respond within 30 days. If the response is not satisfactory, the organizations – similar to the procedure described above – receive a certified warning letter requiring the organization to indicate within a 30 day period how it has addressed the concerns. If those are not resolved within the 30 days the organization is moved to the "inactive" list and the case is being referred to the FTC or DoT. It was confirmed that even if the case was resolved within the 30 days the DoC could refer it to the FTC.

21. As an example, the DoC indicated that Facebook and Cambridge Analytica were for instance removed from the list for some processing because they lapsed.

22. In addition, the DoC clarified that concerning the Facebook data breach, the certificate to the Privacy Shield of Facebook does not cover the platform from which the app accessed the data.

23. The DoC has also designated 1 person to follow the media and to do keyword searches to identify possible breaches of the Privacy Shield commitments.

24. The DoC also performs regular checks for broken links to the privacy policy on the Privacy Shield list.

25. The DoC has not made use of its right to request a copy of the relevant privacy provisions of an organizations contract with an agent.

26. **European Commission and EDPB representatives' presentations** The European Commission, EDPB Chair and representatives gave a short presentation on the updates about the work done on the European Union side.

1.3 Oversight and supervision of compliance with the principles - Activities by the FTC

27. FTC now has 5 commissioners again.

28. The new commission is organizing hearings on Competition and Consumer Protection in the 21st Century which will also cover the existing and possible extension of the FTC´s enforcement powers (https://www.ftc.gov/policy/advocacy/public-comment-topics-process#5).

29. In the Division of Privacy and Identity Protection, Bureau of Consumer Protection there are 40 lawyers working only on privacy (a few also work on FOIA) and there are more people from other fields (e.g. tech) that support their work.

30. This year the FTC has brought 5 new Privacy Shield cases: 2 against organizations that did not complete their certification, 3 cases where the certification has lapsed. In most of those cases, the organization failed to verify the deletion, return or continued application of the Privacy Shield Principles to personal data transferred under the Privacy Shield.

31. The FTC has started to send out CIDs (Civil Investigation Demands) proactively to monitor compliance with the Privacy Shield Principles. The FTC could not provide more details on the selected targets or topics of this exercise. In general the FTC has a broad latitude to do sweeps. There is no need for the

FTC to demonstrate that it has a reasonable suspicion. The objective is rather to identify where it is profitable to spend the resources.

32. The FTC still practices the already established procedure to check the cases it investigates for other reasons if the organization is also certified under the Privacy Shield.

33. With regards to the ongoing investigation concerning Facebook and Cambridge Analytica, the FTC was not in a position to share any detail. However, the Chief Council of the DoC shared verbally the content of an early response letter from Facebook in which the company basically presented different points of its line of defence.

1.4 Oversight and supervision of compliance with the principles - Activities by the DoT

34. Currently there is no airline participating in the Privacy Shield and only very few ticket agents.

35. Because the DoT`s situation is very similar to the one of the FTC it looks closely at FTC practice and case law. The DoT has not received any Privacy Shield related complaints so far.

1.5 Guidance for the companies adhering to the Privacy Shield

36. The DoC has (following informal consultation of members of the ITS at working level) produced guidance on the Accountability for Onward Transfer Principle and the notion of Processor and published it on its website

1.6 IRM

37. The DoC has issued guidance to the IRM in order to have comparable annual reports.

38. The DoC plans to issue guidance on possible conflicts of interest for the next year.

39. Most complaints to the IRM VeraSafe were found ineligible because the complainant was an U.S. resident and the company concerned was also situated in the U.S.

40. As contractually agreed, if there was a breach in the Privacy policy (meaning if the company did not respect its privacy policy, not that the policy itself is in breach of the Privacy Shield), the VeraSafe clients (organizations that certified under the privacy shield) committed to accept VeraSafe's decision to impose a "fine" on them. The "fine" would be paid to the individual that successfully claimed a breach.

1.7 Arbitral Panel

41. The fee, that according to the Privacy Shield text is collected from the certified organizations annually is actually only collected once at the initial certification. The collected amount (under Safe Harbor and the Privacy Shield) totals to 4.5 million $.

42. Arbitral panel procedure has never been triggered so far. The question is if the fee should still be collected. Recommendation of the Arbitral Administrator Association (that manages the fund) is to not change anything for now since there is no figure on how much the handling of an average case would cost.

1.8 Automated Decision Making

43. The COM presented the main elements of a study commissioned to an independent contractor.

44. The study came to the conclusion that automated decisions making (in the narrow GDPR definition of decisions having legal effects on individuals), these decisions are not taken on the basis of data transferred from the EU. Such decisions are more likely to take place in "EU customer facing" situations (i.e. where the US company directly targets EU customers).

45. However, the study at the same time underlines that this is a fast developing area which has to be closely monitored in the future.

46. In the rare situation where ADM are made (for example in the context of credit lending, housing, employment), cases where personal data transferred from the EU are used is quite limited.

47. Some private companies who participated in the joint review exercise (such as Workday and Salesforce) confirmed that they are offering services to their customers (EU businesses) which can be AI-based and potentially conduct some automated decisions[29]. However, these companies insisted that in any case they always act as data processors under the instructions of data controllers based in the EU.

48. According to the study, several credit-reporting agencies have self-certified under Privacy Shield (notably Experian, one of the three big major reporting companies in the US). The FTC has general enforcement jurisdiction over these agencies, in cooperation with the US Consumer financial bureau, which has supervisory authority over credit-reporting agencies (such companies have different products - some of these products may fall under the US Fair Credit Reporting Act). The Consumer financial bureau would pass on cases to the FTC so the same principles apply to such companies and if they are misrepresented the FTC would enforce them.

49. FTC publicly announced that they are investigating Equifax.

50. The US FTC presented the case about "Realpage", a background screening company doing criminal checks which was conducting automated decisions making by using weak accuracy verification methods (if the last name and the first three letters of the firstname of an individual matched a criminal record, Realpage would consider this enough to identify the individual as criminal). The FTC asked the company to put in place a better, reasonable procedure to ensure firstnames' accuracy. The case led to a 3 million dollars fine settlement[30].

51. There was no other significant new developments as regards Automated Decision Making to take note of.

1.9 HR Data

52. Since the work on guidance regarding the processing of employment data within the last year was not successful this year's review focused less on the definition of HR data but rather on the consequences the different definitions lead to: The worry on the EU side being, that additional protections granted by the Privacy Shield for employment data (Opt In in marketing purposes rather than opt out) would

[29] See for example the "Prism Analytics" tool offered by Workday which allows companies to "bring data in at scale from any source and prepare, analyze and securely share it with[in the] organization" (see https://www.workday.com/en-us/applications/prism-analytics.html) and the AI-based predictive marketing tool "Einstein" proposed by Salesforce (see: https://www.salesforce.com/products/einstein/overview/).
[30] See: https://www.ftc.gov/enforcement/cases-proceedings/152-3059/realpage-inc

not fall under anyone's jurisdiction. Given the wording of the Privacy Shield, the discussions on different possible readings of this need to continue.

2 ON GOVERNMENT ACCESS TO PERSONAL DATA: RELEVANT DEVELOPMENTS IN THE U.S. LEGAL FRAMEWORK AND TRENDS

53. Legal framework has not changed substantially.

2.1 Reauthorisation of 702 FISA

54. The U.S. government reported about the amendments authorized by the FISA Amendments Reauthorization Act of 2017.

55. In particular, further explanation was provided about the possibility to reintroduce "about collection". It was stressed that, if the governments were to re-introduce "about collection" under the UPSTREAM programme, it would be required to take particularly demanding procedural steps (implying authorizations by the Court and the Congress), and where the FISA Court would be expected to appoint an amicus curiae when such an application is made.

56. The U.S. government also reported about the several transparency requirements, including semi-annual reports, which – together with additional material – is made available on a new website: https://www.intel.gov/intel-vault.

2.2 PPD-28

57. The U.S. government published a response to the recently published (in redacted form) report by the PCLOB. It disagrees with the PCLOB on the question of whether the scope of application of PPD28 is sufficiently clear for the agencies to apply it (PCLOB expressing doubts in the said report).

58. The U.S. government confirmed that the safeguards of PPD-28 also apply for personal data collected under 702 FISA. This would include safeguards related to the retention of data, their dissemination, and specifications on the targeting with regard to the purpose of collecting foreign intelligence.

2.3 The Ombudsperson mechanism and the EU individual complaint handling body

59. Acting Under Secretary of State for Economic Growth, Energy, and the Environment and Acting Privacy Shield Ombudsperson, Manisha Singh, explained the procedures set up to make the Ombudsperson mechanism under the Privacy Shield work, including how a case would be handled in theory. No further declassified information was shared as to the rules of procedure of how she cooperates with the intelligence community. She assured she would not sign a response letter to the requestor if she were not convinced of the findings presented to her. It was confirmed during the discussion that, in response to an Ombudsperson request, she would be provided with a report from the Intelligence Community (IC) in order to provide oversight and to take actions (without being able to directly access information or directly remedy non-compliance). She also stressed that she would have the ability to escalate the matter to the Secretary of State in order to assure that her demands are met.

60. The European Centralised Body (EUCB) presented its rules of procedure, explaining how a request would be handled before submitted to the Ombudsperson.

61. A representative of the Intelligence Community (IC) confirmed that the Inspector General of the ODNI would always be informed when a request would be forwarded to the ODNI by the Ombudsperson.

62. As the remedying of a possible violation, the U.S. government clarified that any violation of FISA would also have to be reported to the FISA court.

2.4 PCLOB

63. Shortly before the second annual review, the Senate confirmed three members of the PCLOB. As President Trump appointed those candidates on 16 October 2018, the PCLOB has reached quorum again. Two additional candidates have been nominated and are awaiting their confirmation by the U.S. Senate.

64. In addition, also shortly before the joint review, the PCLOB published a redacted version of its report on PPD-28. The government also published a response to that report.

65. The new PCLOB will have to decide about the declassification of report on Executive Order 12333 finalized under the previous PCLOB Chair.

66. As regards other reports to be done, and possible reviews of previous report, such as on section 702, the new PCLOB would have to determine in the coming times its work plan and schedule.

2.5 Inspector General (IG) of the ODNI

67. The new IG was sworn in on 17 May 2018. He stressed his independence and the fact that he has full access to (classified) documents in the IC community, which would as a matter of fact never be restrained.

68. He clarified that usually indirect access to information would be sought through reports from the IC community, but that the IG has direct access as well, if needed.

69. He also confirmed that IG, in principle, has discretion whether to act and would follow set priorities, but that requests by the Ombudsperson would in the current setting always be considered as of particular importance.

2.6 Redress

70. The U.S. government presented recent case law of the FISA court and referred to the website of the FISA court, where redacted decisions are published.

71. Related to the procedural requirement of "standing", the U.S. government reported about the ACLU case, decided by different FISA "chambers" and finally on the appellate level. It deals with an unusual case, where ACLU was seeking the publication of FISA court decisions, based on a right of public access to documents. The court had denied in the first instance that ACLU would have standing. Finally, the FISA Court of Review court said it would.

72. No further developments could be presented on the requirement of standing in other relevant cases, as the Wikimedia case is still pending. With regard to legal claims relying on a violation of FISA, the U.S. Government referred to the possibility of making a Freedom of Information (FOIA) request first.

73. The U.S. confirmed that PPD-28 does not create rights enforceable before a court. Consequently, cases would have to be brought to the attention of the IG or the Ombudsperson.

2.7 Additional information on access to data by law enforcement authorities

74. The U.S. government reported about a Department of Justice memo on the Stored Communications Act[31]. The purpose of the memo would be to further harmonize the use of such applications to the court which prohibit providers to disclose the order. According to the new memo, such applications have to be further justified by the prosecutors seeking such order, and a general limit of 1 year for such orders is foreseen, with exceptions that need to be justified again.

75. The U.S. government also reported about the Supreme Court ruling in the Carpenter case, in which a suspect was prosecuted on the basis cellphone location records, without a search warrant. The Supreme Court ruled that the evidence was illegally acquired and not receivable in court, since the suspect had a reasonable expectation of privacy for these data so that the government had violated the Fourth Amendment to the United States Constitution by accessing the cellphone location records without a search warrant. [32]

[31] Stored Communications Act (SCA, codified at 18 U.S.C. Chapter 121 §§ 2701–2712) is a law that addresses voluntary and compelled disclosure of "stored wire and electronic communications and transactional records" held by third-party internet service providers (ISPs).
[32] Carpenter v. United States, 138 S. Ct. 2206



EU - U.S. Privacy Shield - Third Annual Joint Review

Adopted on 12 November 2019

Table of contents

1 Executive summary 4
1.1 Introduction 4
1.2 On the commercial aspects of the Privacy Shield 4
1.3 On the access by public authorities to data transferred to the U.S. under the Privacy Shield5
1.4 Conclusion 7
2 Introduction 9
3 On the commercial aspects of the Privacy Shield 10
3.1 Guidance for the companies adhering to the Privacy Shield 10
3.2 Clear and easily available information for EU individuals 11
3.3 Self-(Re)Certification Process and Cooperation between U.S. authorities in the Privacy Shield mechanism 11
3.4 Oversight and supervision of compliance with the Principles – Activities of the DoC 13
3.5 Oversight and supervision of compliance with the Principles – Activities of the FTC 14
3.6 Independent Recourse Mechanisms 15
3.7 HR Data 15
3.8 Automated-decision making/Profiling 16
4 On the derogations to the Privacy Shield to allow access to data for Law Enforcement and National Security purposes 17
4.1 Introduction 17
4.2 Collection of data (under section 702 and under EO 12333) 17
4.2.1 Collection of data for national security purposes under Section 702 17
4.2.2 Collection of data for national security purposes under Executive Order 12333 18
4.2.3 Safeguards provided in Presidential Policy Directive 28 (PPD-28) 18
4.3 Oversight 19
4.4 Redress for EU individuals 20
4.5 Ombudsperson mechanism 20
4.6 Access to data for law enforcement purposes 22
5 Conclusion 22
ANNEX TO THE EDPB REPORT ON THE SECOND EU-US PRIVACY SHIELD ANNUAL JOINT REVIEW 24
General Information 24
1 On commercial aspects 24
1.1 Self-Certification Process and Cooperation between U.S. authorities in the Privacy Shield Program 24
1.2 Oversight and supervision of compliance with the principles - Activities by the DoC 25
1.3 Independent Recourse Mechanism (IRM) 27
1.4 Arbitral Panel 27
1.5 Oversight and supervision of compliance with the principles - Activities by the FTC 27
1.5.1 Concerning the status of the Privacy Shield enforcement in general 27
1.5.2 On the Facebook case which led to the recent settlement with the FTC (follow-up of the discussions in the second Joint Review and update on this case) 28
1.5.3 On the general developments in US privacy law that may affect the Privacy Shield and on the resources of the FTC 28
1.6 Oversight and supervision of compliance with the principles - Activities by the DoT 29
1.7 Onward Transfers 29
1.8 Automated decision-making/Profiling 30
1.9 HR Data 30
1.10 US domestic privacy update: NIST Framework 30
2 On government access to personal data: relevant developments in the U.S. legal framework and trends 30
2.1 Ombudsperson mechanism 30
2.2 Inspector General (IG) 31
2.3 PCLOB 31
2.4 ODNI and Department of Justice presentation and Q/A on government access to personal data: relevant developments in the U.S. legal framework and trends 32
List of abbreviations 34

The European Data Protection Board

Having regard to Article 4 and Recitals 145 to 149 of the Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield ("EU - U.S. Privacy Shield),

HAS ADOPTED THE FOLLOWING REPORT:

1 EXECUTIVE SUMMARY

1.1 Introduction

1. According to the EU–U.S. Privacy Shield adequacy decision ("Privacy Shield")[1] adopted on 12 July 2016, **eight representatives of the EDPB participated in the third joint review conducted by the European Commission, on September 12 and 13 of 2019** in Washington to assess the robustness of its adequacy decision and its practical implementation.

2. Based on the concerns elaborated in the previous opinions of the WP29 and of the EDPB, in particular opinion 1/2016, and the reports following the first and second joint review, the EDPB focused on the assessment of both the **commercial aspects** of the Privacy Shield and on the **government access to personal data transferred from the EU for the purposes of Law Enforcement and National Security, including the legal remedies available to EU individuals.**[2] The EDPB assessed once again whether these concerns have been addressed and also whether the safeguards provided under the EU-U.S. Privacy Shield are workable and effective.

3. The European Commission published its report of the third joint review on October 23, 2019.

4. **The EDPB's main findings concerning this third joint annual review**, stemming both from written submissions and from oral contributions are hereby presented in this report.

1.2 On the commercial aspects of the Privacy Shield

5. The third annual review showed that the U.S. authorities have continued their efforts to implement the Privacy Shield.

6. The **DoC as well as the FTC also undertook new ex officio oversight and enforcement actions as regards the compliance of Privacy Shield certified organizations** with the requirements under the Privacy Shield. The EDPB particularly welcomes that the DoC has increased the number of "random spot checks" to 30 organizations per month.

7. **However, one of the main concerns already expressed by the WP29 and the EDPB remains a certain lack of oversight in substance.** Indeed, the checks performed by the DoC are principally focused on formal aspects. The enforcement actions by the FTC focused on procedural violations of the framework rather than on the substance. **This lack of substantial checks thus remains a concern of the EDPB as, even taking into account discretionary and limited investigations by the FTC, a majority of companies' compliance with the substance of the Privacy Shield's principles remains unchecked, although many of them were introduced or further detailed compared to the Safe Harbor. In addition, the increase of complaints, in general, although resolved successfully, does not entirely compensate for this lack of proactive checks on substance. Indeed, these complaints do not seem to concern the issues of concerns underlined by the EDPB so far as they seem to mainly focus on procedural aspects.**

8. **One example for which the EDPB sees the need for more substantive checks are onward transfers.** Since onward transfers possibly lead to transfers of data outside of the jurisdiction of U.S. and EU authorities with possibly no data protection provided by law it is of utmost importance that the competent US Authorities closely monitor the practical implementation of the Privacy Shield's "Accountability for the Onward Transfers Principle". As a first step, for example the DoC could make use of its right to ask organizations to produce the contracts they have put in place with third countries' partners in order to assess whether those provide the necessary safeguards and to discover if any further guidance or other action by the DoC or the FTC is needed.

9. **Another area that requires further attention is the application of the Privacy Shield requirements regarding HR Data.** While the EU Supervisory authorities remain available to exchange with the US Authorities, the discussions on this issue will have to continue between the European Commission and the US Authorities given the different possible readings of the wording of the Privacy Shield. In parallel, the Commission is still called upon to address this issue and clarify the text in order to avoid that possible different interpretations lead to gaps in the protection of EU data subjects.

10. **Also, the re-certification process needs to be further refined**. The situation of outdated listings leads to avoidable confusion that should be addressed also in the interest of concerned Privacy Shield certified organizations.

11. Last but not least, the EDPB recalls the **remaining issues** with respect to certain elements of the commercial part of the Privacy Shield adequacy decision as already raised in the WP 29's Opinion 01/2016 in particular regarding the absence or the limitation to the rights of the data subjects (i.e. right to object, right to access, right to be informed for HR processing), the absence of key definitions, the application of the principles when it comes to "processors", the lack of guarantees on transfers for regulatory purpose in the field of medical context, the lack of specific rules on automated decision making and the overly broad exemption for publicly available information. Those remain valid.

1.3 On the access by public authorities to data transferred to the U.S. under the Privacy Shield

12. The EDPB **welcomes the appointments of the last missing members of the Privacy and Civil Liberties Oversight Board (PCLOB), enabling it to be fully functioning and operational, as well as its increased transparency concerning its work plan.**

13. **The EDPB also welcomes the appointment of Mr Keith Krach, as "permanent" Ombudsperson on 18 January 2019**.

14. Despite these developments, **some of the main points of concern, already expressed by the WP29 and the EDPB in this area in their previous reports, still have to be fully resolved**.

1 Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, OJ L 207, 1.8.2016, p.1.

2 Any reference to the "EU" shall be understood as a reference to the "EEA", in accordance with Decision of the EEA Joint Committee No 154/2018 of 6 July 2018 and Decision of the EEA Joint Committee No 144/2017 of 7 July 2017.

15. More specifically, the c**ollection and access of personal data for national security purposes** under both Section 702 of FISA[3] and Executive Order 12 333[4] still remains an important issue for the EDPB.

16. In this respect, the EDPB recalls that it continues to consider that within the surveillance programs, more specific safeguards would be needed, e.g. for precise targeting to determine whether an individual or a group can be a target of surveillance and for stricter scrutiny of individual targets by an independent authority ex-ante.

17. In addition, although it acknowledges the efforts that the PCLOB has undertaken to follow-up on its past recommendations concerning section 702 FISA, as well as to issue a new report on the FBI's querying of data under Section 702, **the EDPB deeply regrets that the PCLOB will not issue further reports** on PPD-28[5] to follow up on the first report in order to provide additional elements as to how the safeguards of PPD-28 are applied, as well as a general updated report on Section 702 FISA, especially since it was reauthorized with few adjustments since the last Joint Review. The EDPB indeed recalls, as the WP29 did before, that reports of the PCLOB were very useful to feed the assessment led by the WP29 and by the EDPB and would in particular be useful to assess whether the collection of data under Section 702 is not indiscriminate and access is not conducted on a generalized basis under the UPSTREAM program, and for assessing the necessity and proportionality of the definition of "targets", the tasking of selectors under **Section 702** (including in the context of the **UPSTREAM program**[6]), as well as the concrete process of application of selectors in the context of the UPSTREAM program to clarify whether massive access to data occurs in this context. Concerning the application of **Executive Order 12 333** to EU data transferred to the U.S., the EDPB will welcome the finalization by PCLOB of its awaited reports on EO 12 333. However, as the EDPB understands that these reports will most likely remain classified, they may not be used as a relevant source of information on the concrete operation of this Executive Order and on its necessity and proportionality.

18. Access to such reports **would allow the EDPB to provide a comprehensive assessment of these aspects**. It consequently stresses that, in order to perform more meaningful reviews, it could benefit from accessing to additional documents and discussing additional classified elements, following the examples of PNR or TFTP reviews.

[3] See the Foreign Intelligence Surveillance Act (50 U.S.C. § 1801 et seq.) (FISA) – its section 702 allows for data to be collected from non-U.S. persons reasonably believed to be outside the United States in order to obtain foreign intelligence information (50 U.S. Code §1881a (D)(1))

[4] See footnote 59 of the Privacy Shield Adequacy Decision: "E.O. 12333: United States Intelligence Activities, Federal Register Vol. 40, No 235 (8 December 1981). To the extent that the Executive Order is publicly accessible, it defines the goals, directions, duties and responsibilities of U.S. intelligence efforts (including the role of the various Intelligence Community elements) and sets out the general parameters for the conduct of intelligence activities (in particular the need to promulgate specific procedural rules). According to Sec. 3.2 of E.O. 12333, the President, supported by the National Security Council, and the DNI shall issue such appropriate directives, procedures and guidance as are necessary to implement the order."

[5] "PPD-28 is a directive of the President of the United States laying down consistency principles with which signals intelligence collection shall be authorised and conducted but PPD-28 is not a legal basis for collection" – See Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision of the WP 29 as well as annex VI of the Privacy Shield Decision

[6] See WP29 report on the Privacy Shield of 28 November 2017 (page 15): "Two programs are confirmed to be operating under Section 702 of FISA: PRISM and UPSTREAM. (…)Under PRISM, the relevant U.S. authorities require internet service providers to provide them with the data of their users corresponding to "selectors", once "tasked" by the competent authority.
Under the UPSTREAM program, the providers of the telecommunication backbone are required to assist the NSA by identifying and collecting transiting data "to" and "from" a chosen "selector" in the flow of communications between communication service providers."

19. Due in particular to the problematic admissibility threshold of the **"standing requirement**", the redress by EU citizens before U.S. courts is still to be effectively guaranteed. Therefore, the EDPB will continue to follow closely the evolution of the case law.

20. Hence, the independence of the Ombudsperson remains a key element, as this institution is designed to compensate the uncertainty in seeking effective redress before the court, if not the lack thereof.

21. During the third annual review, it was clarified that any violation of the targeting and minimisation procedures under Section 702 FISA would be reported to the FISC by the Ombudsperson, in which case the FISC may decide to issue a deficiency order. Despite further discussions on the procedural aspects of the (inadmissible) first case referred to the Ombudsperson by the EU Centralized Body earlier this year, as well as on hypothetical cases which brought some clarifications, the exact powers of the Ombudsperson still need to be clarified, through the **declassification of internal procedures** concerning the interactions between the Ombudsperson and the other elements of the intelligence community or oversight bodies. Based on the information provided so far, the EDPB is of the view that the Ombudsperson's access to information, which appears to remain indirect, and its powers to remedy non-compliance vis-à-vis the intelligence authorities, are still not sufficient in the light of Article 47 EU Charter of Fundamental Rights. It also underlines that the Ombudsperson is not in a position to bring a matter before the court other than to bring a violation of Section 702 FISA to the attention of the FISC.

22. Finally, regarding the **access to data for law enforcement purposes,** the EDPB underlines its remaining concerns on the available effective remedies for individuals in cases where the personal data processed by companies are accessed by law enforcement authorities.

1.4 Conclusion

23. The EDPB **welcomes the efforts made by the U.S. authorities and the Commission to implement the Privacy Shield, especially ex officio oversight and enforcement actions, as well as the appointments of the last missing members of the PCLOB and of a permanent Ombudsperson.**

24. However, **the EDPB still has a number of significant concerns that need to be addressed by both the Commission and the U.S. authorities**.

25. **As regards the commercial aspects, the absence of substantial checks remains a concern of the EDPB. Other areas that require further attention are the application of the Privacy Shield requirements regarding onward transfers, HR data and** the application of the principles when it comes to **processors, as well as the recertification process. More generally, the members of the Review Team would benefit from a broader access to non-public information, concerning commercial aspects and ongoing investigations.** In addition, the EDPB recalls the **remaining issues** with respect to certain elements of the commercial part of the Privacy Shield adequacy decision as already raised in the WP 29's Opinion 01/2016.

26. As regards the **collection of data by public authorities**, **the EDPB can only encourage the PCLOB to issue and publish further reports. It regrets** that on Section 702 FISA no general report is contemplated, to provide an assessment of the changes brought since the last reauthorization in 2018. **The EDPB would be very interested on an additional report on PPD-28 to follow up on the first report** including an assessment of how the safeguards of PPD-28 are applied Finally, the EDPB underlines the importance of reports on Executive Order 12 333, and regrets that those reports will most likely remain classified. In this regard, the EDPB stresses that the members of the review team only have access to the same documents as the general public. **The EDPB recalls that the security cleared experts of the**

EDPB remain ready to review additional documents and discuss additional classified elements, in order to have **more meaningful reviews**, following the example of PNRs or TFTP reviews.

27. **On the Ombudsperson mechanism**, despite some new elements provided during this year's review, especially on the procedural aspects in relation to the first case submitted to the Ombudsperson but declared inadmissible, as well as on hypothetical cases, **the EDPB is still not in a position to conclude that the Ombudsperson is vested with sufficient powers to access information and to remedy non-compliance. Thus, it still cannot state that the Ombudsperson can be considered an "effective remedy before a tribunal" in the meaning of Art. 47 of the EU Charter of Fundamental Rights**.

28. Finally, the EDPB recalls that the **same concerns will be addressed by the Court of Justice of the European Union in cases that are still pending** before it.

2 INTRODUCTION

29. On 6 October 2015[7], the European Court of Justice invalidated the Safe Harbor adequacy decision after having recalled the important role played by the protection of personal data in the light of the fundamental right to respect for private life and the large number of persons whose fundamental rights are liable to be infringed where personal data is transferred to a third country not ensuring an adequate level of protection. Soon after, the Commission started negotiations for a new adequacy decision and presented a draft adequacy decision with its annexes.

30. On the 13 April 2016, the Working Party 29 issued an opinion[8] on the draft new adequacy decision aiming at replacing the invalidated Safe Harbor. On the same day, the WP29 also issued a working document[9] on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees).

31. On 30 May 2016, the European Data Protection Supervisor also issued an Opinion on the draft adequacy decision[10].

32. On 12 July 2016, the European Commission adopted the EU-U.S. Privacy Shield adequacy decision[11] ("Privacy Shield"), which has also been incorporated into the EEA Agreement[12]. The Privacy Shield entrusts the Commission with the task to assess the findings of the adequacy decision, including on the basis of the factual information collected in the context of an Annual Joint Review[13]. Important concerns on both the commercial aspects and aspects relating to government access to personal data transferred under the Privacy Shield for the purposes of Law Enforcement and National Security had then to be addressed and further assessed in the context of the Joint Review.

33. In addition, it is also foreseen in recital 147 of this adequacy decision that the Commission will meet a number of US authorities, and that the "*participation in this meeting will be open for EU DPAs and representatives of the Article 29 Working Party*".

34. The WP 29 also issued a report following the first Joint Review of the Privacy Shield in November 2017[14] as well as a second report following the second Joint Review in January 2019[15].

35. The third Joint Review of the Privacy Shield took place on the 12 and 13 September 2019 in Washington D.C. Eight representatives of the EDPB, a Commissioner as well as experts at staff level, were

7 Case C-362/14
8 WP 238 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf
9 WP 237 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp237_en.pdf
10 EDPS Opinion 4/2016 of 30 May 2016: https://edps.europa.eu/sites/edp/files/publication/16-05-30_privacy_shield_en.pdf
11 Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, OJ L 207, 1.8.2016, p.1.
12 Decision of the EEA Joint Committee No 144/2017 of 7 July 2017 – Recital (1): "the Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (1) is to be incorporated into the EEA Agreement".
13 See recitals 145-149 and Article 4(4) of the decision.
14 WP 255: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48782
15 EU - U.S. Privacy Shield - Second Annual Joint Review - Adopted on 22 January 2019

designated to be part of the Review Team ("the Review Team") that accompanied the Commission during this two-day meeting with U.S. authorities, companies' representatives, NGOs and a representative from the binding arbitration mechanism.

36. In advance to the Joint Review, the Commission sent questionnaires to US trade associations representing Privacy Shield certified organizations and NGOs, as well as a detailed agenda to organize the discussions with the US authorities and stakeholders during the Joint Review itself. The EDPB sent contributions to take part to the elaboration of these documents.

37. Right before the Joint Review, the Commission and the Review Team met with some of the NGOs to further discuss their input on the Privacy Shield.

38. Also, briefly before the actual Joint Review took place in Washington, the EU-Supervisory Authorities representatives were contacted by the DoC to informally discuss the existing divergences on the interpretation of the notion of HR Data (see I. 7.)

39. The new factual elements presented by the US authorities companies' representatives, NGOs and by a representative from the binding arbitration mechanism participating in the Joint Review, stemming both from written submissions, as well as from oral contributions during the Joint Review itself, are presented in annex to this document. They were presented at the EDPB Plenary on 8 October 2019.

3 ON THE COMMERCIAL ASPECTS OF THE PRIVACY SHIELD

3.1 Guidance for the companies adhering to the Privacy Shield

40. The EU-U.S. Privacy Shield is an adequacy decision that was designed to frame transfers of personal data outside the protections provided under GDPR to ensure the level of protection of natural persons guaranteed by GDPR is not undermined in the absence of a general law in the US providing for an essentially equivalent level of protection of personal data. It is of utmost importance that there is a common understanding of the text to ensure the application in the receiving State will correspond to the requirements for such transfers as set out under EU data protection law. It has to be ensured that this text is interpreted correctly and that organizations and individuals on both sides of the Atlantic are "on the same page" as regards their duties and rights under the Privacy Shield.

41. Thus, in the report of the first annual review the WP 29 emphasized the need for clear guidance on the application of the Privacy Shield principles. In the second year of operation of the framework and following informal consultation of members of the ITS at working level, the DoC has issued **guidance in the form of FAQs on the Accountability for Onward Transfer Principle**[16] **and the notion of Processor**[17] and published it on its website. In the third year of operation of the framework the DoC issued one more guiding document also in the form of FAQs on the Privacy Shield and the UK aiming at issues related to Brexit. The EDPB has not been involved in any way in the drafting of these new FAQs.

42. Since the last joint review, not much additional guidance was published by the US authorities. In this regard, the EDPB recalls in particular that guidance concerning processors may further specify the application of the principles when it comes to processors ("agents").[18]. Also, the use of Standard Contractual Clauses as a tool for onward transfers remains to be examined.

43. The EDPB still regards the issuance of guidance as a good start and expects that in the future there will be more guidance as to other key elements. In previous reports, the EDPB already suggested to further work for example the **Choice Principle** (on when and how a data subject can opt out from the processing of his/her data for a new purpose), or on the **application of the Notice Principle** (more specifically on the timing for certified organizations to give notice to individuals). In addition, it recalls that a **clarification of the scope of the right of access** could be helpful to prevent misunderstandings. In its last report, worries regarding the possibly very narrowly interpreted duty to grant the right of access only to data that is "stored" by an organization voiced by the WP 29 still remains valid.

3.2 Clear and easily available information for EU individuals

44. The WP 29 had found that to complement the specific information provided in concrete cases by the companies themselves, the US authorities should strive to offer **more information in an accessible and easily understandable form to the individuals regarding their rights and available recourses and remedies.**

45. The Privacy Shield website already had a specific section named "EU and Swiss individuals" containing subsections "My rights under Privacy Shield" and "Privacy Shield participants list"[19] where individuals were informed about their rights. The various possibilities to lodge complaints were also explained and partly supported by direct links. After the first annual review and as a response to the WP 29s suggestions the DoC added a one-page document to their website that gives individuals an overview[20] of the program with a strong focus on the individual's rights and how they can be exercised. The EDPB acknowledges the efforts made by the DoC to provide further guidance for EU individuals on the Privacy Shield website. Although the number of complaints slightly increased since the last report, it remains difficult to determine whether this is directly linked to this guidance. The EDPB will thus remain watchful.

3.3 Self-(Re)Certification Process and Cooperation between U.S. authorities in the Privacy Shield mechanism

46. After having noted improvements in the certification process in the report of the second Joint Review, the EDPB did not identify any relevant change of the procedures in the third Joint Review:

47. The DoC still reviews all self-certifications (both for first time applicants and for recertification submissions) and checks:

    1. Registration with an Independent recourse mechanism (IRM) company
    2. Payment of Annex I Arbitral Fund Contribution

16 https://www.privacyshield.gov/article?id=Onward-Transfer-Principle-FAQs (last accessed on 18 December 2018)
17 https://www.privacyshield.gov/article?id=Processing-FAQs (last accessed on 18 December 2018)

18 that the guidance could for example further elaborate on the following details: Notice to be provided by processors needs to be in line with the contract in place between the processor and the controller; that access to data and a Choice mechanism could be provided to the individual directly by the processor provided however that the controller has in the first place authorized the processor to do so; and that for a processor compliance with the Data Integrity and Purpose Limitation principle requires it to process the data only in accordance with the instructions from the controller and on the other hand to implement the appropriate measures as instructed by the controller to assist the later in complying with the data integrity principle.
19 See: https://www.privacyshield.gov/Individuals-in-Europe (last accessed on 27 November 2018)
20 See: https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t0000000QJdq (last accessed on 14 December 2018)

3. Compliance with Privacy Shield supplemental principle 6 (on access to personal information)
4. Completion and consistency of certification information
5. Privacy notices (the existence of all 13 elements required by the Privacy Shield is checked also in the organizations Privacy Policy)

48. Also, the DoC still asks the organizations for more precise links provided for the Privacy Shield listing so individuals can more easily exercise their rights and for more than one point of contact within the organization to make sure messages from the DoC are received. The DoC also checks the applications for inconsistencies between the privacy policy and the certification (For example HR/NON HR).

49. When the DoC refused to list an organisation on the Privacy Shield list, either for first-time certifications or re-certifications, it underlined that it was because the requirements set out by the Privacy Shield were not fulfilled. This indicates that the decision made by the DoC whether or not to list an organization on the Privacy Shield website is – as far as the checks go - not a rubber stamp exercise.

50. However, on the basis of the information given by the US authorities during the joint reviews, those checks still do not go into the substance of the principles. **This absence of substantial checks remains a concern for the EDPB on the general question of sufficient oversight regarding the substance of the Privacy Shield principles.**

51. Following the criticism expressed by the WP 29, the DoC still prohibits a first-time applicant from making public representations about participation until the Privacy Shield Team approves its certification and instead requires an applicant to submit a draft privacy policy for review. It also directs an applicant to remove any premature references of their participation in the Privacy Shield program from their website.

52. **Regarding the re-certification process**, already the second annual review revealed that due to the procedures established by the DoC there are cases where the due date displayed on the Privacy Shield List is already passed while the organization still is listed as an active participant. This occurs when an organization has submitted their recertification but the process is not finalized before the due date. In the third review this was further explored and it was discovered that the process of recertification could take up to 105 days starting at the actual due date. During this whole period of time the organizations will stay on the "active" list.

53. As long as the organizations still publicly commit to apply the Privacy Shield Principles this might not lead to a gap in the protection of individuals. **However the EDPB reiterates that it is the reasonable expectation of individuals who consult the Privacy Shield list that all organizations listed as "active" have current and valid certification checked by the DoC. The EDPB is of the opinion that the change of practice to already set a new due date on the Privacy Shield list as soon as the recertification documents are submitted to the DoC does not lead to the result that only fully checked certifications are displayed as "active" on the List. The EDPB still asks the DoC to explore what can be done to avoid this situation** (especially what can be done to guarantee that there is no gap in the protection of individuals) **and in the meantime to add some explanation for concerned individuals and EU based organizations using the Privacy Shield as a transfer tool so the situation is sufficiently clear to individuals and also organizations within the EU that would like to transfer personal data to a Privacy Shield certified organization and therefore check the validity of the certification on the Privacy Shield List**.

54. During the course of the third Joint review it was also discovered that on the Privacy Shield list there were 29 Organizations listed as "active" that had a due date in 2018. **The EDPB asks the DoC to implement procedures that make sure that the "active" list of participants is always up to date and to implement checks that avoid such outdated listings.**

3.4 Oversight and supervision of compliance with the Principles – Activities of the DoC

55. In the first Joint Review report the WP 29 criticized that the **oversight of the commercial aspects of the Privacy shield mainly relied on the third party companies providing Independent Recourse Mechanisms (IRMs)** and that the **implementation** of the Privacy Shield framework **lacked sufficient oversight and supervision of compliance in practice**. Because the Privacy Shield is a program based on self-certification, it is of utmost importance that U.S. authorities involved in the administration of the Privacy Shield devote sufficient resources at oversight and enforcement activities. The WP 29 considered that the **performance of compliance reviews** of organizations having self-certified to the Privacy Shield is a key element for the effective functioning of the framework and that **ex-officio investigations have to be conducted both by the DoC and the FTC/DoT** to ensure that self-certified organizations concretely implement the requirements of the Privacy Shield.

56. The second review showed that the U.S. authorities (namely DoC and FTC) had made significant efforts to address this concern:

- On a quarterly basis the DoC conducts "false claims reviews" in order to identify organizations that have started but not finished an initial or re-certification or that did not submit their annual re-certification at all.

  The identified organizations receive a certified letter from the DoC, warning them of potential referrals to the FTC or DoT if they do not fulfil outstanding requirements or withdraw properly from the program. The DoC informs the FTC/DoT of its intent to send those letters. The organizations have 30 days to respond to the letter. The DoC compiles a list of those organizations that fail to take action and respond to the letter. This procedure has led to 100 referrals from the DoC to the FTC, 56 of those referral were made in the second year of the Privacy Shield program. DoC and FTC/DoT cooperate throughout the whole process. Simultaneously with the referral an organization is (at least temporarily) removed from the "active" Privacy Shield List.

- As foreseen in the Privacy Shield text, the DoC also performs random web searches for false claims of participation in the program. Those web-searches have only led to few cases that were referred to the FTC.

- The DoC has performed a sweep of 100 randomly chosen organizations. The focus of the sweep was the accessibility of the Privacy Policy, the responsiveness of the organization and the availability of the IRM. The DoC sent more in-depth compliance questionnaires to 21 organizations that showed minor or more significant peculiarities (for example: No response from the designated point of contact; the Privacy policy was no longer accessible online; Missing references to one or more elements of the notice principle). The organizations must respond within 30 days. If the response is not satisfactory, the organizations – similar to the procedure described above – receive a certified warning letter requiring the organization to indicate within a 30-day period how it has addressed the concerns. If those are not resolved within the 30 days, the organization is moved to the "inactive" list and the case is being referred to the FTC or DoT.

- The DoC has also designated 1 person to follow the media and to do keyword searches to identify possible breaches of the Privacy Shield commitments.
- The DoC also performs regular checks for broken links to the privacy policy on the Privacy Shield list.

57. This year, the DoC indicated that it issued more than 670 warning letters, most of them regarding false claim participation.

58. Aside from the fact that the DoC has increased the amount of random spot checks to 30 randomly chosen organizations per month, the third Joint Review did not reveal any further developments in this direction.

59. **Therefore, while the EDPB still welcomes all these steps taken by the DoC to ensure formal compliance with the Principles of the Privacy Shield because they remain a good starting point; the EDPB is deeply concerned that these checks still remain focused on the formalities to be complied with rather than on the substance. The EDPB urges the DoC to extend the oversight activities also to substantial elements, such as the purpose limitation principle for instance.**

60. Further to monitoring concrete compliance with all principles of the framework, **one of the areas that would need particular attention in this context remains the area of onward transfers.** The DoC has still not made use of its right to request a copy of the relevant privacy provisions of organizations contracts with their agents. **Since onward transfers possibly lead to transfers of data outside of the jurisdiction of U.S. and EU authorities with possibly no data protection provided by law it is of utmost importance to closely monitor the practical implementation of the Accountability for the Onward Transfers Principle.**

3.5 Oversight and supervision of compliance with the Principles – Activities of the FTC

61. In last year's review the EDPB noted an increase in the FTC´s activities regarding the enforcement of the Privacy Shield. This year however, the FTC recognized that due to its lack of budget, it had to prioritize its actions with regards to the enforcement of Privacy rules.

62. While last year the FTC has brought 5 new Privacy Shield cases: 2 against organizations that did not complete their certification and 3 cases where the certification has lapsed. In most of those cases, the organization failed to verify the deletion, return or continued application of the Privacy Shield Principles to personal data transferred under the Privacy Shield. The FTC indicated that some investigations into potential Privacy Shield violations remain ongoing, without further clarifying their scope and the exact number of cases. This year the FTC has brought 7 new cases regarding the enforcement of the Privacy Shield, still on administrative failures and not on the substance of the Privacy Shield's principles. The EDPB stresses that further controls concerning onward transfers could be led, given that the solutions put in place by the certified companies are not checked by the DoC either.

63. In the Division of Privacy and Identity Protection, Bureau of Consumer Protection there are 40 lawyers almost exclusively working only on privacy. They are supported by for example technical experts.

64. The FTC investigates Privacy Shield-related referrals (143 discovered "false claim cases" in the third year) but in most cases by the time these referrals arrive to the FTC they have been solved in the meantime so many cases fall out.

65. Concerning the Facebook settlement reached since last year's joint review, the FTC clarified that the scope of it remains outside the scope of the Privacy Shield as none of the products covered by the settlement were certified under the Safe Harbor or the Privacy Shield[21].

66. **The EDPB still welcomes any ex officio activity to proactively monitor compliance with the Privacy Shield Principles undertaken by the FTC. It nevertheless regrets the low number of cases concerning the enforcement of the Privacy Shield and that the FTC still was unable to share any more detail on its approach as this leaves the EDPB unable to have a clear insight on the concrete activities and cases, and therefore to be in a position to assess how and to what extent the FTC ensures compliance monitoring with the substance of the Privacy Shield's principles.**

3.6 Independent Recourse Mechanisms

67. The independent dispute resolution providers reported an overall increase in both the number and complexity of the complaints received under the Privacy Shield framework since the second joint review. The EDPB acknowledges that the number of complaints slightly raised and were resolved in a timely manner. However, the increase of complaints in general do not entirely compensate for the lack of proactive checks from the competent US authorities. Indeed, from the feedback collected during the Joint Review, the complaints do not seem to concern the issues of concerns underlined by the EDPB so far as they seem to mainly focus on procedural aspects.

68. In the report of the second annual joint review, the EDPB expressed its expectation to see improved and comparable reports provided by the IRM services that also explain how possible conflicts of interests are precluded. The DoC reported that it has developed guidance to the IRMs in order to avoid possible conflicts of interests, and updated its guidance on Annual IRM report to include potential conflicts of interest and the description of how they avoid such situations. However, the guidance developed and standardized forms issued do not cover all aspects of the reports. In particular, the EDPB found that no standardised template format for the reports have been introduced yet on this aspect. In order to ensure full comparability, the EDPB therefore recommends the DoC to introduce a standardized template format for the Annual IRM report, which also contains explanation on how possible conflicts of interests are precluded.

3.7 HR Data

69. As already stated in the previous reports, the notion of HR data in the context of the Privacy Shield is interpreted differently within the EU and by the US authorities. Although the DoC initiated the producing of guidance regarding the processing of HR data, including through informal consultation of members of the WP 29 and of the EDPB later on, on working level in this regard, the work on this guidance was not successful yet due to the absence of convergence on the definition of the notion of HR data. Last year's review thus focused less on the definition of HR data but rather on the consequences, the different definitions within the EU and by US authorities may lead to. On the EU side, the concern is that additional protections granted by the Privacy Shield for employment data (opt-in to marketing purposes rather than opt out) would not and could not be enforced by any U.S or EU authority. The EDPB recalls that in its understanding, HR data should be protected in the same way whether they are processed by the employer or by a processor, including concerning the choice and

21 The effects of the immunity of the settlement reached however remained unclear. Indeed, this immunity would not prevent individuals to bring actions against facebook for other products, or for practices which were unknown at the time of the settlement. However, should facebook adhere to the Privacy Shield in the future for the products covered by the settlement, without changing anything from its commitments, it is still to be clarified whether the immunity derived from the settlement would cover corresponding violations of the Privacy Shield in this context for the practices covered by the settlement.

purpose limitation principles. While the EU Supervisory authorities remain available to exchange with the US Authorities, the discussions on this issue will have to continue between the Commission and the US Authorities given the different possible readings of the wording of the Privacy Shield. **In parallel, the Commission is still called upon to address this issue and clarify the text in order to avoid that possible different interpretations lead to gaps in the protection of employees in the European Union.**

3.8 Automated-decision making/Profiling

70. In the report of the first annual review, the WP29 called upon the Commission to contemplate the possibility to provide for specific rules concerning automated decision making to provide sufficient safeguards including the right to know the logic involved and to request reconsideration on a non-automated basis, especially after having explored the extent of the practical relevance of automated decision making processes by Privacy Shield certified companies if the analysis generates an actual need for additional safeguards.

71. As part of the second review the Commission presented the main elements of a study[22] commissioned to an independent contractor regarding the existence of automated decision-making on the basis of personal data that has been transferred from the EU to Privacy Shield certified companies in the US. While the authors of the study highlight a series of challenges for conducting this work (limited availability of experts on the topic and reservations to take part in interviews, limited relevance of answers in certain cases, opacity characterizing the data industry on such practices notably), the main conclusion that can be drawn from the study is that automated decisions (in the narrow GDPR definition of decisions having legal effects on individuals or similarly significantly affecting them) are not taken on the basis of data transferred from the EU. According to the study, such decisions are more likely to take place in "EU customer facing" situations (i.e. where the US company directly targets EU customers).

72. However, the study at the same time underlined that this is a fast developing area which still has to be closely monitored in the future, therefore this issue was also discussed at the third annual joint review.

73. In their reply to the questionnaire sent by the Commission in preparation to the third joint review, one trade association reported that member companies that employ automated decision-making included information about this in their policies and maintain mechanisms to allow consumers to exercise control, such as the ability to contest an automated decision and seek human review.

74. During the third joint review, the FTC confirmed that the U.S. adheres to the OECD Recommendation on AI [adopted on 22 May 2019].

75. The FTC specified that companies are not required to provide the right to know the logic involved and to request reconsideration on a non-automated basis under the Privacy Shield (and therefore, to include a reference in this regard in the privacy policy submitted pursuant to the Privacy Shield). If companies do commit themselves to provide these rights, but then, contrary to this commitment, they do not provide them, this will constitute a misrepresentation, against which the FTC can take enforcement action. In the area of consumer credit, the FTC referred to the Fair Credit Reporting Act (FCRA).

76. **Based on the findings of the third joint review, the EDPB is on the opinion that it is important that the Commission continues monitoring cases related to automated decision making and profiling and to contemplate the possibility to foresee specific rules concerning automated decision making to provide sufficient safeguards, including the right to know the logic involved and to challenge the decision obtaining human intervention when the decision significantly affects him or her**.

22 See: https://ec.europa.eu/info/sites/info/files/independent_study_on_automated_decision-making.pdf (last accessed on 19 December 2018)

4 ON THE DEROGATIONS TO THE PRIVACY SHIELD TO ALLOW ACCESS TO DATA FOR LAW ENFORCEMENT AND NATIONAL SECURITY PURPOSES

4.1 Introduction

77. **Since the second Joint Review, the US legal framework has not substantially changed.**

78. Consequently, some of the main points of concern that the WP29 and the EDPB expressed in their previous opinions, in the area of access to data transferred under the Privacy Shield for national security or law enforcement purposes, have not been fully resolved. These **main concerns are related to the collection of data, to oversight, to judicial redress and finally, to the Ombudsperson mechanism. This calls for a reminder of the EDPB's analysis.**

79. **In addition,** this year's joint review took place at the time the "Schrems II" case, also concerning the Privacy Shield, is pending before the CJEU (the Court held the hearings on this case on 9 July 2019).

80. Also taking this background into account, specific points were discussed with the U.S. authorities during the Privacy Shield Review (*See infra*, in particular concerning PPD28, when data are collected outside the US).

4.2 Collection of data (under section 702 and under EO 12333)

81. As recalled in the previous reports, the CJEU underlined in its Schrems judgment[23] that the "*protection of the fundamental right to respect for private life at EU level requires derogations and limitations in relation to the protection of personal data to apply only in so far as is strictly necessary*"[24] and ruled that "*legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter*"[25].

82. **The previous concerns expressed therefore remain relevant,** as the legal framework has not significantly changed on any of the aspects concerning the collection of data from the perspective of EU individuals (and non-US persons). Therefore, the EDPB recalls the concerns expressed in this respect in the two previous reports.

4.2.1 Collection of data for national security purposes under Section 702

83. The EDPB stresses once again the need for independent assessment on the necessity and proportionality of the definition of "targets" and of the concept of "foreign intelligence" under section 702 FISA (including in the context of the UPSTREAM program), and maintains its call for further independent assessment of the process of application of selectors in specific cases ("tasking of selectors"). It also maintains its call for further clarification in the context of the UPSTREAM program to exclude that massive and indiscriminate access to personal data of non-U.S. persons takes place.

23 Case C-362/14, 5 October 2015
24 See recital 92, See also cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger, recital 52.
25 See recital 94.

84. With regard to 702 FISA, it was clarified during the discussions of this year's Review that a "person" to be identified as a target could refer to several individuals using the same identifier, provided that all these individuals would be non-U.S. persons and fulfill the applicable criteria for being targeted[26].

85. **The EDPB welcomes that the now fully functional Privacy and Civil Liberties Oversight Board (PCLOB), as an independent oversight agency, has decided "to review the FBI's querying (searching) of data obtained pursuant to Section 702" as well as the fact that the PCLOB indicated it would follow-up how the previous recommendations expressed in their report concerning section 702 were taken into account. However, it regrets that PCLOB does not intend to prepare and issue an updated general report on Section 702, building on the report issued in 2014, especially given that since then section 702 was reauthorized. A general updated report would help provide an assessment of the new provisions inserted in Section 702 in the context of its reauthorization, as well as on the practice of other agencies than the FBI, in particular intelligence agencies.**

4.2.2 Collection of data for national security purposes under Executive Order 12333

86. **In the context of the third Joint Review, given the disagreements between the EDPB and the US authorities as to the relevance of Executive Order 12333 for the adequacy decision, the application of Executive Order 12333 was still not further discussed.**

87. As underlined in the previous reports, the EDPB maintains the WP29 long-standing position that the analysis of the laws of the third-country for which adequacy is considered, should not be limited to the law and practice allowing for surveillance within that country's physical borders, but should also include an analysis of the legal grounds in that third country's law which allow it to conduct surveillance outside its territory as far as EU data are concerned. Necessary limitations to governmental access to data should extend to personal **data "on its way" to the country, for which adequacy is recognized**. The EDPB recalled this position before the CJEU[27]. During the previous Joint Reviews, the U.S. authorities underlined that Executive Order 12333 could not be used as a basis for collection of data inside the U.S. territory and that they consider that collection of data under this Executive Order falls outside the scope of the Privacy Shield.

88. Once again, given the uncertainty and unforeseeability of how EO 12333 is applied, the EDPB stresses the importance of the awaited PCLOB's reports on this text. However it understands that they are likely to remain classified, so that no further information on the concrete operation of this Executive Order and on its necessity and proportionality would become available neither to the public, nor to the Review team of the EDPB.

4.2.3 Safeguards provided in Presidential Policy Directive 28 (PPD-28)

89. The U.S. authorities confirmed once again their commitment to comply with the rules set in the Presidential Policy Directive 28 (PPD-28). The EDPB welcomes this commitment. At the same time, the EDPB stresses that the PPD-28 provides for the only safeguards and limits to the collection and use of data collected outside the U.S., as the limitations of FISA or other more specific U.S. law do not apply. These limitations mainly concern the collection of data, as the signal intelligence activities have to be as "tailored as feasible".

90. **No new substantial discussion took place in the context of the third joint Review, concerning the interpretation and application** of the six purposes allowing for the use of data foreseen in this Directive, or relating to the amount of personal data collected by the U.S., that would allow a validation

26 For instance, this could cover for a couple using the same email address or the members of an organization using the same communication app account.

27 At the hearing organised on the 9 July 2019 in the so-called Schrems II case (C-311/18)

of the commitments and the assurances provided by U.S. authorities. In the context of this year's Joint Review, discussions mainly focused on the interpretation and application of the additional ground (situation/scenario) for bulk collection foreseen by the first sentence of footnote 5 of Section 2 PPD-28[28], which provides that "*The limitations contained in this section do not apply to signals intelligence data that is temporarily acquired to facilitate targeted collection.*" The U.S. authorities explained the meaning of "*signals intelligence data that is temporarily acquired to facilitate targeted collection*". The EDPB understood from these discussions that this footnote means that data may be collected in bulk - and regardless of the six purposes foreseen in Section 2 - if collected temporarily, with a view to establishing an identifier for a defined target. This would thus be an additional ground to collect data in bulk, and in this case general principles of Section 1 of PPD-28 would still apply. The EDPB regrets that the notion of "temporarily" could not be further specified, as in the EDPB's understanding, it appeared to mean that as long as the target has not been identified, bulk collection could continue.

91. The EDPB also recalls that a more detailed follow-up report on how the key terms of the PPD-28 are practically understood and applied in the different surveillance programs would be welcome, since it could provide additional information clarifying these aspects.

92. In addition, although the U.S. authorities claimed that Executive Orders and Presidential Policy Directives have "the force of law", the EDPB recalls that in the context of the previous Joint Reviews, it was also clarified that these violations of the instruments can never be - in themselves - relied upon for an action by an individual before a Court. Therefore, it would not be possible for an EU individual to directly invoke the violation of PPD-28 safeguards to bring an action before a U.S. Court.

4.3 Oversight

93. The EDPB recalls that comprehensive **oversight of all surveillance programs** is crucial, which the CJEU and the ECtHR have also emphasized in the respective jurisprudence.

94. Already during the two previous annual Joint Reviews, the oversight activities of several entities were presented. The EDPB considered that a **comprehensive oversight structure** is in place, composed of different elements that are in part, independent from the Intelligence Community, including the Privacy and Civil Liberty officers, the Inspector Generals, the PCLOB, the FISC and Congress, amongst others.

95. **The EDPB welcomes the appointment of the last missing members of the PCLOB. The PCLOB is now fully functioning and operational. The PCLOB also presented, for the first time, its work program, and the EDPB welcomes this step in terms of transparency from this oversight body.** As emphasized before, the EDPB considers the PCLOB, whose recommendations have been an important contribution to reforms in the U.S. and whose reports have been particularly helpful to understand the functioning of the various programs, as an independent body, an essential element of the oversight structure. The EDPB calls again for public reports to be published, including on crucial aspects of the U.S. legislation such as the three reports (one of which only is already finalized) on EO 12333, especially since the functioning of this piece of legislation could never be discussed during the joint reviews. In this context, the EDPB also regrets that, although the PCLOB indicated it would follow-up how the previous recommendations expressed in their report concerning section 702 were taken into account (see supra as well), no general updates of previous reports will be prepared, be it on Section 702 FISA or on PPD-28. Furthermore, the EDPB recalls that in the context of joint reviews organized for other EU instruments such as for PNR agreements or for the TFTP agreement, members of the Review Team are

28 Which applies only to Executive Order 12 333 and not to Section 702 FISA, which does not allow bulk collection.

given access to more information than the general public. However, in the case of the Privacy Shield joint reviews, the members of the review team only have access to the same documents as the general public. They recall that they remain ready to review additional documents and discuss additional elements under security clearance, in order to have more meaningful reviews.

4.4 Redress for EU individuals

96. As already highlighted in the previous reports, the EDPB underlines that in its Schrems ruling, the CJEU stressed the importance to have a right to an effective remedy before a tribunal[29]. A third-country can only be considered as providing an adequate level of protection in accordance with the GDPR, where EU individuals have access to an independent and impartial redress body, including in surveillance matters.

97. **As the U.S. government informed during this year's Joint Review that the legal framework is unchanged and no significant new case law concerning these matters needed to be considered, the EDPB recalls its position and the relevant criteria to take into account when assessing the level of adequacy are still those stemming from the jurisprudence of the CJEU and ECtHR**.

98. As repeatedly stressed in the previous reports, while the APA and FISA appear to provide limited grounds for an EU individual to challenge surveillance in U.S. courts, the principal problem appears to concern the **"standing requirement"**.

99. Under the procedural requirements as currently interpreted by the U.S. courts, it appears to be difficult and uncertain that an EU individual could satisfy the procedural requirement of standing when bringing a suit concerning a surveillance measure on the basis of section 702 FISA or EO 12333. The EDPB will therefore continue to follow closely the evolution of these cases as they could trigger the establishment of new additional guarantees having a positive impact on the effectiveness of judicial redress offered to EU individuals before U.S. courts. However, as was confirmed during the Joint Reviews, the interpretation of the notion of "standing" in surveillance matters is evolving with cases still pending[30].

4.5 Ombudsperson mechanism

100. **In the context of the third Joint Review, the EDPB welcomed the nomination of Mr Keith Krach, on 18 January 2019, as "permanent" Ombudsperson**

101. The **Ombudsperson** mechanism aims at complementing the possibilities of redress. More critically, it might be argued that it is meant to compensate for the uncertainty or unlikeliness to seek effective redress before a U.S. court in surveillance matters. The WP29 therefore welcomed the establishment of the Ombudsperson, as this could constitute a significant improvement in terms of protection of the rights and freedoms of EU individuals with regards to U.S. intelligence activities. In addition, it was confirmed that the PPD-28 does not create enforceable rights for the individuals (see supra). The Ombudsperson mechanism provides the only way for EU individuals to ask for a verification that the relevant authorities have complied with the requirements of this instrument by asking the Ombudsperson to refer the matter to the competent authorities, which include the Inspector General, to check the internal policies of these authorities.

102. Having regard to Article 47 of the Charter of Fundamental Rights of the European Union, the threshold for independence and impartiality required in a redress mechanism such as the Ombudsperson is high.

29 See paragraph 95
30 See in particular cases ACLU v. Clapper, and Wikimedia v. NSA.

Having analysed the jurisprudence of the ECtHR in particular, the WP29, in its Opinion of 13 April 2016, and the EDPB assessed the Ombudsperson mechanism in their opinions and in previous reports, and suggested that the appointment of a high-ranking official in the Department of State as the Ombudsperson, who can be dismissed at any time without notice, is problematic having regard to aforesaid requirements of independence and impartiality[31].This concern is also raised by the designation, as Ombudsperson, of Mr Keith Krach, given the fact that he is the Under Secretary of State for Economic Growth, Energy, and the Environment.

103. In addition, the EDPB recalls that during the first and the second Joint Reviews, as well as before the EDPB Plenary in July 2018, the previous Ombudsperson and the U.S. government explained in some detail the important work done in order to ensure that requests would be handled lawfully and efficiently. The previous Ombudspersons also stressed that they needed to be convinced of the findings before responding to the request and underlined that they could escalate the issue should they be unconvinced by the outcome presented to them following the assessment of a request. These aspects were confirmed by the new Ombudsperson, who also underlined his personal commitment to only sign letters to close cases when convinced that they had been dealt with in a proper way. While the EDPB still has no reason to doubt the integrity of the new Ombudsperson, **it recalls its expectation to learn more about the powers of the Ombudsperson vis-à-vis the Intelligence Community**. This information still remains partial. The procedures governing the access to relevant information by the Ombudsperson and governing the interactions of the Ombudsperson with the other members of the Intelligence Community, including the oversight bodies, remain partially classified.

104. As the first case referred to the Ombudsperson mechanism since the second Joint review was eventually declared inadmissible because it concerned data transferred outside the scope of the Privacy Shield, the case has not allowed to further discuss in detail how cases are handled under the procedures in place after the preliminary assessment of the admissibility of a case.

105. Nevertheless, the staff of the Office of the Ombudsperson explained in abstract how an admissible case would be handled. In this context, it was explained that violations of Section 702 FISA would also be reported to the FISC, which may decide to issue deficiency order to have it remedied within 30 days.

106. Questioned about his role in the Ombudsperson mechanism, the Inspector General for the Intelligence Community ("IG") confirmed that the first complaint sent to the Ombudsperson was shared with him, and that more generally in the context of requests sent by the Ombudsperson, he would, depending on the circumstances of the case, refer it to the competent intelligence agency, and that a remedy could be proposed to the ODNI. It was recalled that in case of an acknowledged incident, collection stops, the underlying information has to be purged, and, if any reports were based on that information, these reports must be recalled (this is a standard procedure for reports in this domain). He added that Congress would also be informed about recommendations and about cases where the recommendation is not followed through. Further, the IG explained that the Ombudsperson would also be informed of the findings and recommendations to the ODNI necessary for the Ombudsperson to perform his duties. Nevertheless, the IG confirmed that in his report to the Ombudsperson, he could remove information from the report to the ODNI in order to protect sources and other sensitive information. As a consequence, the information shared with the Ombudsperson may not necessarily be identical to the information shared with the ODNI.

107. With regard to the first case under the Ombudsperson mechanism, the EDPB is committed to assess its internal processes in light of the experiences made and to adapt them, if need be.

31 See WP29 Opinion 'European Essential Guarantees', Guarantee C, referring among others to ECtHR, Zakharov.

108. In conclusion, based on the available information, the EDPB still doubts that the powers of the Ombudsperson to remedy non-compliance vis-a-vis the intelligence authorities are sufficient, as his "power" seems to be limited to decide not to confirm compliance towards the petitioner. In the understanding of the EDPB, the Ombudsperson is not vested with powers, which courts or other similarly independent bodies would usually be granted to fulfill their role. Therefore, the EDPB remains unable to hold that the Ombudsperson is vested with adequate powers to effectively exercise its duty. In addition, the EDPB recalls that the decisions of the Ombudsperson cannot be brought to court for judicial review.Therefore, the lack of judicial review of the decisions of the Ombudsperson, and consequently the impossibility to obtain remedies where the Ombudsperson will not provide any answer (failure to act) or provides an unsatisfactory reply to the complainant, still remains a concern. **As a conclusion, the EDPB is not in a position to conclude that the Ombudsperson is vested with sufficient independence, and with sufficient powers to access information and to remedy non-compliance. Thus, it cannot state that the Ombudsperson can be considered an "effective remedy before a tribunal" in the meaning of Art. 47 of the Charter of Fundamental Rights**[32].

4.6 Access to data for law enforcement purposes

109. As regards **access to data for law enforcement purposes**, the EDPB continues to note that the procedural safeguards inherent to the criminal procedure (notably, due process) imply that data are accessed by the competent public authorities for a specific purpose and that the individual concerned is notified if her or his data have been accessed within the framework of a criminal proceeding, in the context of which they can raise objections to the collection and use of such data and have access to judicial redress.

110. However, the EDPB recalls the concerns - already expressed in the previous opinion issued by the WP29[33]- regarding the availability of effective remedies to the individuals concerned in cases where the data processed by companies is accessed by law enforcement authorities[34].

5 CONCLUSION

111. The EDPB **welcomes the efforts made by the U.S. authorities and the Commission to implement the Privacy Shield, especially ex officio oversight and enforcement actions, as well as the appointments of the last missing members of the PCLOB and of a permanent Ombudsperson.**

112. However, **the EDPB still has a number of significant concerns that need to be addressed by both the Commission and the U.S. authorities**.

113. **As regards the commercial aspects, the absence of substantial checks remains a concern of the EDPB. Other areas that require further attention are the application of the Privacy Shield requirements regarding onward transfers, HR data and** the application of the principles when it comes to **processors, as well as the recertification process. More generally, the members of the Review Team would benefit from a broader access to non-public information, concerning commercial aspects and ongoing investigations.** In addition, the EDPB recalls the **remaining issues** with respect to certain elements of the commercial part of the Privacy Shield adequacy decision as already raised in the WP 29's Opinion 01/2016.

114. As regards the **collection of data by public authorities**, **the EDPB can only encourage the PCLOB to issue and publish further reports. It regrets** that on Section 702 FISA no general report is contemplated, to provide an assessment of the changes brought since the last reauthorization in 2018. **The EDPB would be very interested on an additional report on PPD-28 to follow up on the first report** including an assessment of how the safeguards of PPD-28 are applied Finally, the EDPB underlines the importance of reports on Executive Order 12 333, and regrets that those reports will most likely remain classified. In this regard, the EDPB stresses that the members of the review team only have access to the same documents as the general public. **The EDPB recalls that the security cleared experts of the EDPB remain ready to review additional documents and discuss additional classified elements**, in order to have **more meaningful reviews**, following the example of PNRs or TFTP reviews.

115. **On the Ombudsperson mechanism**, despite some new elements provided during this year's review, especially on the procedural aspects in relation to the first case submitted to the Ombudsperson but declared inadmissible, as well as on hypothetical cases, **the EDPB is still not in a position to conclude that the Ombudsperson is vested with sufficient powers to access information and to remedy non-compliance. Thus, it still cannot state that the Ombudsperson can be considered an "effective remedy before a tribunal" in the meaning of Art. 47 of the EU Charter of Fundamental Rights**.

116. Finally, the EDPB recalls that the **same concerns will be addressed by the Court of Justice of the European Union in cases that are still pending** before it.

32 A first request from an EU individual was received under the Ombudsperson mechanism at the end of 2018.
33 See WP 238.
34 Concerning access to data for law enforcement purposes, we also pointed out, supra, at Section 2.1 of this Report/Conclusions, to the possible access (querying) by law enforcement authorities to data acquired under Section 702 FISA.

ANNEX TO THE EDPB REPORT ON THE SECOND EU-US PRIVACY SHIELD ANNUAL JOINT REVIEW

Factual findings of the third annual joint review of the EU-US Privacy Shield

GENERAL INFORMATION

1. The U.S. Delegation was composed of high level representatives.
2. As of now, the Privacy Shield List contains around 4984[35] organizations, 509[36] are on the "Inactive" List either because they have voluntarily withdrawn from the program (39 in the last year), not submitted their recertification in a timely manner or because their recertification has been initiated but not completed in a timely manner. There was no case where an organization was removed from the List because it persistently failed to comply.
3. Of the participating Organizations 70 - 75% are small and medium size organizations with less than 250 employees. 96% of the participating organizations certified for non-HR data transfers, 33% for HR transfers. The main businesses certifying are: Information and Communications Technology, Business and Professional Services, Media and Entertainment, and Education.

1 ON COMMERCIAL ASPECTS

1.1 Self-Certification Process and Cooperation between U.S. authorities in the Privacy Shield Program

4. The DoCs method and scope of checks in the initial review of a certification and the recertification has not changed substantially since the last review. The DoC reviews all self-certifications (first time applicants as well as recertification submissions) for:
    1. Registration with IRM
    2. Payment of Annex I Arbitral Fund Contribution
    3. Compliance with supplemental principle 6
    4. Completion and consistency of certification information
    5. Privacy notices
5. DoC has rejected 9 first time certifications in the last year because the applicants were not eligible to participate in the Privacy Shield because they were not under the jurisdiction of FTC or DoT (5 non-U.S., 4 non-profit organizations).
6. Also, there were no significant changes reported as regards the depth of the analysis the DoC performs: the DoC checks the applications for inconsistencies between the privacy policy and the certification (For example HR/NON HR). It does not check if the data transferred is necessary and proportionate to the purpose for instance because they consider that the Privacy Shield does not go into this level of detail, nor do they check in substance the compliance with other principles.

[35] See https://www.privacyshield.gov/list on 24 September 2019
[36] See https://www.privacyshield.gov/inactive on 24 September 2019

7. In order to address the concern expressed by the WP29 regarding the duty of the certifying organization to publish their privacy policy referring to the Privacy Shield certification before the DoC has completed the exercise of checking and listing the organization, the DoC has changed the procedure.
8. The DoC:
    - Prohibits a first-time applicant from making public representations about participation until the PS Team approves its certification
    - Requires an applicant to submit a draft privacy policy for review
    - Directs an applicant to remove any premature references
9. As the practical experience with the certification process increases, the DoC still uses the same guidance for the review of applications regarding the identification of foreign entities; they ask the companies for more precise links to their privacy policies so individuals could more easily exercise their rights, they ask for more than one point of contact within the organization to make sure messages from the DoC are received.
10. In addition to the 2-weeks-notice of the upcoming deadline to recertify organizations already sent out before the second annual review, the DoC now also sends a reminder one month and one week before the recertification is due.
11. The organizations that want to stay in the Privacy Shield program are obliged to communicate their re-certification by the due date. The DoC stated in the third annual review that organizations that fail to do so within 30 days after the due date are "automatically" moved to the "inactive" list.
12. Since August 2019 the DoC has changed their practice and changes the "Next Certification Due Date" on the Privacy Shield list as soon as any documents for recertification arrive at the DoC.
13. In the course of the 3rd annual review the participating representatives of the EDPB submitted a list of organizations whose recertification due date lay in the past. For 29 of those organizations the due date dated back to 2018. Checks of that list performed on September 25, 2019 led to the result that the DoC moved 87 of those organizations to the "inactive" list. Two organizations disappeared from the whole list. 213 remained on the "active" list.
14. As regards guidance, the DoC has published new guidance material for organizations to address questions around Brexit. The review team is not aware that this guidance was created in cooperation with EU SAs or the EDPB.

1.2 Oversight and supervision of compliance with the principles - Activities by the DoC

15. The DoC still identifies on a quarterly basis organizations that have started but not finished an initial or re-certification or that did not submit their annual re-certification at all.
16. If organizations do submit the paperwork necessary for recertification, the DoC foresees a timeslot of 45 days in which the recertification should be finished. If this is not the case and at least further action to complete the process is not taken by the organization, the DoC sends it a warning letter explaining that if the required action is not taken within a period of another 30 days, the organization will be removed to the "inactive" list and referred to the FTC or DoC.

17. As foreseen in the Privacy Shield text, the DoC still performs random web searches for false claims of participation in the program.

18. In the last year the DoC referred 143 discovered false claims cases to the FTC.

19. After the DoC has performed a sweep of 100 randomly chosen organizations in the second year of the Privacy Shield, it has now started in April 2019 to perform 30 of those checks each month. The focus of the sweep is the accessibility of the Privacy Policy, the responsiveness of the organization and the availability of the IRM. In case those checks result in conspicuities (about 20% of the cases) the organizations receive more in-depth compliance questionnaires from the DoC. Through this procedure minor or more significant peculiarities may appear (for example: no response from designated point of contact; privacy policy was no longer accessible online; missing references to one or more elements of the notice principle). The organizations must respond within 30 days. If the response is not satisfactory, the organizations – similar to the procedure described above – receive a certified warning letter (3 in this year) requiring the organization to indicate within a 30 day period how it has addressed the concerns. If those are not resolved within the 30 days the organization is moved to the "inactive" list and the case is being referred to the FTC or DoT. It was confirmed that even if the case was resolved within the 30 days the DoC could refer it to the FTC.

20. In total the DoC has sent out 669 warning letters to participants of the Privacy Shield since October, and 1 100 were sent in total since the beginning of the programme.

21. The DoC still follows the media and does keyword searches to identify possible breaches of the Privacy Shield commitments.

22. The DoC also still performs regular checks for broken links to the privacy policy on the Privacy Shield list.

23. The DoC has still not made use of its right to request a copy of the relevant privacy provisions of an organizations contract with an agent.

24. Besides the Privacy Shield News and Events section on the website of the DoC that covers several kinds of news and also FTC decisions related to privacy in general but there is no dedicated link to Privacy Shield cases of the FTC as described in the text of the Privacy Shield.

25. In relation to the DoC's work in order to ensure that all organizations recertify and finish their work on time but also for the web searches for false claims and any other aspects of their work the DoC mentioned that it works on improving their technical possibilities.

26. The DoC has in various contexts throughout the review also uttered its wish to establish a closer cooperation between the DoC and the EDSA/ representatives of European Supervisory Authorities (for example on outreach and education, possibilities of more substantial checks).

27. The US CIB announced that they would stop managing the fund set up (to cover the costs of the EU informal panel responsible to take care of complaints submitted mostly from employees whose data have been transferred under the Shield) in accordance with the Privacy Shield in 2020. EU Commission and DPAs were approached to help finding a solution but declined any responsibility in managing it.

28. **European Commission and EDPB representatives' presentations** The European Commission, EDPB Chair and representatives gave a short presentation on the updates about the work done on the European Union side.

1.3 Independent Recourse Mechanism (IRM)

29. The DoC reported that it has developed guidance to the IRMs in order to avoid possible conflicts of interests.

30. One IRM explained once again that such a conflict of interest would be avoided by separating the teams providing IRM services and those verifying ex officio compliance with the Privacy Shield framework, both in terms of tasks and staff. Regarding the management of such potential conflicts between the two teams, it reported on having its own department that monitors these conflicts and has not had identified any so far.

31. Potential conflicts of interest must be included in the annual reports of the IRMs, but neither this aspect of the report was standardized nor any standardised template format for the reports have not been introduced yet.

32. In total, the IRMs received 48 complaints under the Privacy Shield framework and reported an overall increase in both the number and complexity of the complaints.

33. However, the IRMs reported that only one-third of the received complaints were eligible under the Privacy Shield. The other complaints were primarily regarding U.S. companies that were not self-certified under the Privacy Shield framework.

34. The majority of the complaints received were related to requests from individuals regarding a change or removal of their personal data, an unsubscription from the organizations services, the disabling of accounts and the contact with a representative from the applicable organization.

35. Another IRM reported that three complaints were successfully resolved, which related to the access principle as well as the improper handling of the notice principle.

1.4 Arbitral Panel

36. The fee that according to the Privacy Shield text is collected from the certified organizations annually is still being collected only once at the initial certification. The collected amount (under Safe Harbor and the Privacy Shield) totals to more than 5 million $.

37. Regarding the arbitral panel procedure, two requests were submitted since the second annual review. Both requests were dismissed as one failed to comply with the steps needed to invoke such an arbitral panel procedure and the other one did not relate to a company that was a Privacy Shield participant.

1.5 Oversight and supervision of compliance with the principles - Activities by the FTC

38. The FTC representative answered the questions of the Commission and the EDPB along the following 3 main categories:

1.5.1 Concerning the status of the Privacy Shield enforcement in general

39. 7 Privacy Shield cases were handled since the last review, to look more into substantive violations of the framework.

40. Two cases concerned the supplemental principle 6 (on the obligation to continue to apply the Privacy Shield to the data collected after withdrawal from the programme). The FTC also focused on supplemental principle 7 (obligation to verify or certify that the company has assessed its compliance with the Privacy Shield).

41. The FTC also performed *ex officio* reviews: 1 case this year, where the company did not comply with this principle 7 (and thus probably with others). The representative of the FTC announced more cases on the Privacy Shield to come.

42. Following a question from the Commission, the FTC answered that it did not focus only on the formal respect of the Privacy Shield, but also on the substance.

1.5.2 On the Facebook case which led to the recent settlement with the FTC (follow-up of the discussions in the second Joint Review and update on this case)

43. Although the representative of the FTC underlined that they could not share much details as the findings have not been made public, it was indicated that eventually the investigation focused on products for which Facebook did not certify under the Privacy Shield (Facebook only certified for two new products, Workplace premium and Ads Measurement). Thus, contrary to what was expected during the second review of the Privacy Shield, the settlement reached does not have a direct link with the Privacy Shield.

44. The FTC clarified that as an effect of the settlement and of the immunity deriving from it, in the future it could only take action against Facebook concerning violations which were unknown at the time of the settlement (for instance, a new complaint on a new subject or concerning a different service). This means that if Facebook adhered to the Shield for these products without any further change, the FTC would probably not be in a position to act and that existing complaints on the aspects covered by the settlement will not be handled further.

45. Concerning the possibility for the FTC to contemplate a repetitive practice, for instance in terms of the exercise of rights of data subjects, as a persistent failure to comply, the DoC indicated that it is a possibility if an organization regularly fails to comply and it is no longer possible to assume that it is limited to an individual case.

46. Questioned about the settlements in general, the FTC indicated that it had to offer the company the opportunity to settle in all privacy cases, when the FTC is ready to open a case before the court. The FTC could refuse to settle, for instance when they have civil penalty. However the FTC would not impose a fine that would make the company go bankrupt. When calculating the amount of money for the settlement, the FTC would have to take into account how much the company earned from its practice and add the amount of the fine, according to the principle that a company shall not profit from its misconduct.

47. For each civil penalty, the FTC underlined that it was required to look at multipliers: degree of guilt, the ability to pay, deterrence and harm to consumers.

48. Concerning the interactions of the FTC with the DOJ in the context of settlements, the FTC stressed that it does not have the power to impose a civil penalty on its own and that in such situation they would have to refer the case to the DOJ, which then has 45 days to either take the case or let the FTC take it back. In case the DOJ takes the case on behalf of the State, the FTC underlined that they usually follow the recommendations made by the FTC.

1.5.3 On the general developments in US privacy law that may affect the Privacy Shield and on the resources of the FTC

49. The representative of the FTC underlined that the Federal Trade Commission's policy is to be aggressive towards companies within the boundaries of the powers they have (i.e., in cases for which the FTC is able to impose civil penalties).

50. Several cases were initiated or finalized this year.

51. The FTC is also continuing its hearing process to improve their orders. This process already resulted in the additional requirement to companies to have their assessor for outside compliance reviews approved. These assessors are also required to provide the FTC with all the documents in their possession.

52. Nevertheless, the FTC stressed its lack of effective means to perform its duties and missions (lack of resources, restricted competence and powers, e.g. with respect to non-profit organisations, etc). In this regard, it was underlined that without further resources, the FTC would not be in a position to process more than 7/8 cases regarding the enforcement of the Privacy Shield per year (although the duration of investigations vary from one case to another). The FTC is continuously advocating for a stronger law on first-time violations, the ability to reach non-profit entities, and for more resources.

53. Questioned on its investigatory powers, the FTC confirmed that they could have access to source codes with the issuance of subpoenas. Regarding the criteria used to prioritize their investigations, the FTC indicated that they try to maximize the yield of their resources. They do not plan "fishing expeditions" in advance, but prefer to collect information from open sources that may make a case. It sets it priority on cases regarding sensitive information (credit, finance, health, children information). The FTC stressed that, in principle, they are not an examination agency. Consequently, they could but do not usually investigate on-site but rather use documentation and interrogatories.

1.6 Oversight and supervision of compliance with the principles - Activities by the DoT

54. The DoT is in charge of the supervision of data processing related to air transportation, which includes two main entities: airline companies, and ticket agents. To date, no airline company is participating in the Privacy Shield, and only very few ticket agents.

55. Because the situation of DoT is very similar to that of the FTC, it looks closely at FTC's practice and case law. The DoT has not received any Privacy Shield related complaints so far.

1.7 Onward Transfers

56. The representatives of DoC underlined that FAQs on how to comply with the Accountability for Onward Transfers Principle, published before the second review, are available on the Privacy Shield website. They contacted law firms, consultancy agencies and other stakeholders to seek more information about their experiences and expectations regarding this issue. These organizations indicated that the negotiation of the clauses on onward transfers are usually part of a wider, general negotiation, in which not only the Privacy Shield principles, but US states law also has to be considered (eg. existing state law requirements on data breach). According to the information gathered as a result of this outreach, the organizations found the FAQs helpful.

57. The DoC does not get specific questions from organization on onward transfers during the certification and re-certification process, applicants usually have more general questions on the interpretation of the Privacy Shield Principles.

58. Questioned about DoC's possibility to request a summary or copy of the contract used by an applicant to comply with the principle on onward transfers, the representatives indicated that they did not make use of this possibility so far. The DoC also indicated that it is not part of the compliance questionnaire and the sweep checks to verify specifically these contracts, and the compliance with the Accountability for Onward Transfers Principle.

1.8 Automated decision-making/Profiling

59. The FTC confirmed that the US adheres to the OECD Recommendation on AI [adopted on 22 May 2019].

60. In their reply to the questionnaire from the review team, one trade association reported that member companies that employ automated decision-making included information about their policies and maintain mechanisms to allow consumers to exercise control, such as the ability to contest an automated decision and seek human review.

61. The FTC specified that companies are not required to provide such rights under the Privacy Shield (and therefore, to include a reference in this regard in the privacy policy submitted pursuant to the Privacy shield). If companies commit themselves to provide these rights but then, contrary to this commitment, they do not provide them, this will constitute a misrepresentation, against which the FTC can take enforcement action.

62. In the area of consumer credit, the FTC referred to the Fair Credit Reporting Act (FCRA).

1.9 HR Data

63. In the course of the review the EDPB review team was approached by the DoC to further discuss this issue. The main topic was the possible loss of European oversight for European employees and their expectation in terms of rights (notice and choice). On the other hand for certain service providers, the DoC underlined that it might be difficult to even know if they are processing employee data. Arguments and possible solutions were exchanged. The DoC took note of those and will contemplate on possible ways forward. There is no concrete outcome of the discussions yet.

1.10 US domestic privacy update: NIST Framework

64. The National Institute of Standards and Technology (NIST) presented the last version of its "Privacy Framework" (preliminary draft, 6 September 2019). The Privacy Framework, customizable by companies, aims at providing guidance to companies on how to reach a certain level of data protection (the process), without pre-setting the level to be reached ("desired privacy outcomes").

2 ON GOVERNMENT ACCESS TO PERSONAL DATA: RELEVANT DEVELOPMENTS IN THE U.S. LEGAL FRAMEWORK AND TRENDS

65. Legal framework has not changed substantially.

2.1 Ombudsperson mechanism

66. During the review, Keith Krach presented himself as the new Under Secretary for Economic Growth, Energy, and the Environment of the U.S. Department of State, and the Privacy Shield Ombudsperson. He stressed that the Ombudsperson mechanism needs to provide an effective, empowered channel of review for EU individuals.

67. He also confirmed to be independent from the Intelligence Community (IC), and stressed, as his predecessors did during the first and second reviews, that he will not sign his name to a letter if he would have any remaining doubts on the completion of appropriate redress.

68. The Ombudsperson's staff then reported that the only request received under the Ombudsperson mechanism was in agreement with the EU Centralized Body found to be deficient.

69. Referring to a hypothetical case, the staff then presented in general terms the procedures and powers of the Ombudsperson, stressing that the Ombudsperson would have access to all information he needs to perform its duties and that all incidents of non-compliance would have to be remedied, including the purging of data. It was also provided that violations of section 702 FISA would be reported to the FISA Court.

70. No further specific information about how the Ombudsperson would cooperate with the IC were shared, as the Ombudsperson reported that those procedures continue to be classified.

2.2 Inspector General (IG)

71. The Inspector General of the IC gave an overview of how IGs are set up and operate within the U.S. government and the U.S. legal system. He stressed that IG's are independent from the bodies they oversee, and that they are empowered by law to review and investigate any abuse of power.

72. The IG reported that the request which was made under the Ombudsperson mechanism (and found to be deficient) was also examined by the office of the IG.

73. The IG confirmed that the office could take up any hint of an abuse of power, also on its own initiative. However, the IG only investigates concrete cases and does not review policy.

74. During the last year, the IG office has not investigated any matter related to the Privacy Shield.

75. Questioned about how the office of the IG would handle an Ombudsperson request, the IG explained that it would depend on the case, but that he may refer to an agency, and that a remedy may be proposed to the ODNI. He added that Congress would also be informed about recommendations and about cases where the recommendation is not followed through.

76. Further, the IG explained that the Ombudsperson would also be informed of the findings and recommendations to the ODNI necessary for the Ombudsperson to perform his duties. In order to protect sources and other sensitive information, in the report to the Ombudsperson, the IG may remove information from the report to the ODNI. As a consequence, the information shared with the Ombudsperson may not necessarily be identical to the information shared with the ODNI.

77. Finally, the IG clarified that his resources are not decided upon by the Government, but by Congress.

2.3 PCLOB

78. The summer before the third annual review, the Senate confirmed the last two members of the PCLOB. The Chair of the PCLOB underlined that the PCLOB is thus now fully staffed for the first time since 2016.

79. The staff has also doubled since the last review, and 7 new projects have been launched. Overall, the PCLOB is now working on 10 projects and also strengthened its knowledge in terms of technology.

80. For the first time, the PCLOB released an agenda of their current projects, which it will update every six months. The PCLOB also published strategic goals for the next three years, among them technology is identified to be the key factor for privacy.

81. The PCLOB representatives recalled the history of the agency and its functioning.

82. Regarding the current projects, the Chair underlined that the Board is currently working on the following issues:

- Regarding NSA's collection of detailed call records under the USA Freedom Act. The report is expected to be finalized later this year.

- Regarding facial recognition in airports, work has started recently.
- Regarding the terrorist watchlist, a project is ongoing as well, yet without any forecast date. It was however underlined that the mere fact of working on a subject already sends a signal.
- Regarding EO 12 333, work is still ongoing:
    a. 3 deep-dive reviews were organized on this subject, 2 of those related to the CIA (1 of them is finalized and transmitted to the Congress), 1 to the NSA (on XKeyscore).
    b. The PCLOB is also providing advice on a range of guidelines on EO 12 333 for internal use.
    c. The PCLOB Chair indicated that they hope some work will be completed and made available in a relative near future.

83. Regarding the calendar of work concerning EO 12 333, the Chair indicated that each deep-dive review can be finalized independently from the others, and be declassified separately. However, the Chair of the PCLOB underlined that in spite of their strong policy towards the broadest dissemination of their works, it was unlikely that these reports would ever be (fully) declassified.

84. Regarding Section 215 and whether their report will be issued by the end this year, the Chair of the PCLOB confirmed that they hope to deliver it in sufficient time, so that it will be available to the Congress in the context of the possible re-authorization of this section.

85. When questioned on whether the PCLOB's report on Section 702 could and would be updated, the Chair of the PCLOB indicated that FBI's access and use of the data would partially be reviewed, but that the PCLOB did not intend to update the whole report.

86. Regarding the mandates the PCLOB gives itself and its work program, the Chair of the PCLOB indicated that the PCLOB has a holistic approach and that its reports focus on collection, but also look at storage, use of data, compliance mechanisms, as well as sharing and dissemination. It was also underlined that the PCLOB's focus evolves where the practice goes, and needs to migrate to those, even when they are not yet known to the public.

2.4 ODNI and Department of Justice presentation and Q/A on government access to personal data: relevant developments in the U.S. legal framework and trends

87. The Chief Privacy Officer of the ODNI confirmed again that the function of his office was to advise on the policies regarding civil liberties and privacy, according to the statues, and that the officers also have the power to conduct investigations, which includes to have access to all the materials and records needed.

88. When performing their missions, they are bound by statutes which govern their actions, by Executive orders, Attorney general's guidelines, Presidential Directives, and orders of courts. This office also provides the public with new interpretations issued by the FISC (either along with the decision or with a summary if the decision itself cannot be provided).

89. The Chief Privacy Officer of the ODNI reported that no major changes took place since the last review. He confirmed that PPD 28 remains in full force and effect.

90. In this regard, he underlined that PPD 28 demonstrates a strong preference to conduct targeted surveillance (as tailored as feasible) rather than bulk, which is, in principle, allowed only for six purposes.

91. He reaffirmed that bulk collection is neither generalised, nor mass collection, and that "bulk collection" is usually a choice, for instance to identify a target.

92. In view of a question raised by the CJEU during the hearing on the Schrems II case, in particular on footnote 5 of PPD 28, after extensive and detailed exchanges, the following elements were clarified:
    - This footnote is not applicable to Section 702 as it is not a bulk collection program (since it is based on the use of selectors). Nevertheless, sections 1, 3 and 4 of PPD 28 apply.
    - This footnote applies to EO 12 333, for instance.
    - This footnote would mean that in addition to the six purposes foreseen under PPD 28 for bulk collection, PPD 28 allows (through this footnote) an additional situation where bulk collection can take place: when bulk collection is temporary, in order to identify a target. In this case, it appears to be possible to derogate from the six other purposes foreseen under PPD 28 to undertake a bulk collection of data, but only temporarily, for another authorized purpose of collection, and in this case, Section 1 of PPD 28 would still apply.
    - Questioned on what "temporary" would mean, the answer was not very clear. It seems that, as soon as the collected data has been processed to help identify the target, useless data is no longer useful is deleted.

93. Concerning targets and selectors under Section 702, the Chief Privacy Officer of the ODNI recalled that the distinction between a selector and a target is important: the target should be a "person", while a "selector" is any communication identifier (e.g., email address, phone number, etc.) allowing to isolate the person's communication data from the bulk. However, questioned on whether a person should necessarily be only one single individual, he acknowledged that in some cases a person could be a group comprising more than one individual (e.g., the users of an email account), provided the size of the group remains limited and that any member of the group needs to have a link with the foreign intelligence at stake and to be a non-US person.

94. The way a person is selected is through the tasking of a selector, which is documented both for approval and oversight.

95. It was stressed that each selector has to be an account used by a person and that it cannot be the name of a person. It has to be a communication account identifier, thus communication always has to be from or to the selector. It was also confirmed that these safeguards related to the tasking of selectors only apply within the framework of Section 702.

96. Questioned on the time limit for which a selector is tasked, it was underlined that a selector is tasked "for as long as it brings back foreign intelligence". Regular checks would thus be performed to confirm that is still useful and necessary.

97. As regards to PRISM and UPSTREAM collection and the filtering of communications, no additional information was presented during this review.

98. At the time of targeting, the NSA shall provide a written explanation to allow for an *ex ante* review in the IC before tasking the selector, as well as a post review by the DoJ. It was recalled that in case of an acknowledged incident, collection stops, the underlying information has to be purged, and, if any reports were based on that information, these reports must be recalled (this is a standard procedure for reports in this domain).

99. In case of an incident, the office of the Privacy Officer would also have to look at the context in which it occurred and to report non-compliance to the FISC (in the context of section 702), with a description of the scope of the incident and of reasons why it happened. The Court then would follow-up on these reports, for instance by determining, in the annual certification process, whether those compliance incidents effectively rendered certification inadequate. It could also issue a deficiency order to have it remedied within 30 days. In addition, quarterly reports on incidents are also sent to the FISC.

100. In addition, the Chief Privacy Officer of the ODNI stressed that semi-annual reports of compliance incidents for the Congress are declassified to the extent allowed and made available on IC on the record, by the DoJ. These reports also show the trends of non-compliance and comments, which provide more useful information than the statistics (see the last one of March 2019).

101. Brief updates were also provided on cases introduced or ruled since the last review concerning FISA §1806 (two cases of the 9th Circuit - Jewel and Fazaga), as well as FOIA (ACLU v. NSA before the appellate court and the following cases, as well as Food marketing Institute v. Argus Leader Media from the Supreme Court).

102. Concerning the Wikimedia case, the DoJ stressed that the first instance considered that the complainants lacked standing, but this judgement was overturned by the appellate court. The case is still pending, while another case was ruled and dismissed on substance, but is being appealed too.

103. Concerning Section 501, for which the Administration is seeking reauthorization of this authority, it was recalled that the NSA is not using it any longer, because the information were too narrow and thus not sufficiently useful.

104. Questioned on how the additional safeguards afforded to the data of EU residents transferred to the US through the Privacy Shield would be reflected in executive agreements concluded between the US and another third country in the context of the Cloud Act, the DOJ indicated that it could not answer this question yet.

LIST OF ABBREVIATIONS

DoC: Department of Commerce

FTC: Federal Trade Commission

IG: Inspector General

APA: Administrative Procedure Act

FISA: Foreign Intelligence Surveillance Act

FISC: Foreign Intelligence Surveillance Court

PCLOB: Privacy and Civil Liberties Oversight Board

PPD-28: Presidential Policy Directive n°28

EO 12 333: Executive Order 12 333

ODNI: Office of the Director of National Intelligence



EDPB Strategy 2021-2023

Adopted on 15 December 2020

Table of contents

1 Introduction 3
2 Pillar 1: Advancing harmonisation and facilitating compliance 3
3 Pillar 2: Supporting effective enforcement and efficient cooperation between national supervisory authorities 4
4 Pillar 3: A fundamental rights approach to new technologies 5

Adopted

1 INTRODUCTION

1. The mission of the European Data Protection Board (EDPB) is to ensure the consistent application of European data protection rules and to promote effective cooperation among supervisory authorities throughout the European Economic Area (EEA).

2. On 25 May 2018, the EDPB began putting into practice a new institutional and legal framework. This framework comprises both the General Data Protection Regulation[1] (GDPR) and the Law Enforcement Directive[2] (LED). Under the GDPR and LED, cooperation is no longer an option or an ancillary task, but a core and integral part of our work. While much has been achieved, we must address a series of challenges in order to enhance the protection of personal data within and beyond our borders. To be effective in confronting the main challenges ahead, the EDPB has decided to define a strategy for 2021-2023.

3. Our ultimate goal of protecting individuals with regard to the processing of personal data continues to drive our actions. The development of a common data protection culture, which serves as an inspiration and model globally, is at the core of our strategy.

4. This Strategy does not provide an exhaustive overview of the work of the EDPB in the years to come. Rather it sets out the four main pillars of our strategic objectives, as well as set of key actions to help achieve those objectives. The EDPB will implement this Strategy within its Work Program, and will report on the progress achieved in relation to each Pillar as part of its annual reports.

2 PILLAR 1: ADVANCING HARMONISATION AND FACILITATING COMPLIANCE

5. The EDPB will continue to strive for a maximum degree of consistency in the application of data protection rules and limit fragmentation among Member States. In addition to providing practical, easily understandable and accessible guidance, the EDPB will develop and promote tools that help to implement data protection into practice, taking into account practical experiences of different stakeholders on the ground.

   - **Key action 1:** the EDPB will focus on providing further guidance on **key notions** of EU data protection law (e.g., on the concept of legitimate interest, on the scope of data subjects' rights) which are essential to its consistent application. Through the organisation of dedicated stakeholder events and public consultations, we will continue to engage with a wide range of external stakeholders (large companies and SMEs, NGOs, DPOs networks and other data

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
[2] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

Adopted

protection professionals) in order to ensure practical relevance. Additional efforts will go to make a more proactive use of the consistency mechanism as well as of other tools in order to address potential gaps or divergences in interpretation and practices in Member States.

- **Key action 2:** the EDPB will further promote **development and implementation of compliance mechanisms for controllers and processors**: increased efforts and resources will be invested – in particular through dedicated workshops and staff trainings - to stimulate the development of tools to promote compliance, in particular codes of conduct and certifications.
- **Key action 3:** the EDPB will foster the development of **common tools** for a wider audience and engage in **awareness raising and outreach activities:** the EDPB already issues guidelines and opinions addressed to professionals with extensive expert knowledge. Building on the resources already available at national level, the Board will develop tools specifically tailored for non-expert professionals, such as SMEs, and for data subjects, in particular children.

3 PILLAR 2: SUPPORTING EFFECTIVE ENFORCEMENT AND EFFICIENT COOPERATION BETWEEN NATIONAL SUPERVISORY AUTHORITIES

6. The EDPB is fully committed to support cooperation between all national supervisory authorities that work together to enforce European data protection law. We will streamline internal processes, combine expertise and promote enhanced coordination. We intend not only to ensure a more efficient functioning of the cooperation and consistency mechanisms, but also to strive for the development of a genuine EU-wide enforcement culture among supervisory authorities.

- **Key action 1**: encourage and facilitate **use of the full range of cooperation tools** enshrined in Chapter VII of the GDPR and Chapter VII of the LED, bridge gaps or differences between national enforcement procedures, and continuously evaluate and improve the efficiency and effectiveness of these tools. Further promoting a common application of key concepts in the cooperation procedure and strengthening of the communication between SAs.
- **Key action 2:** implement a **Coordinated Enforcement Framework** (CEF) to facilitate joint actions in a flexible but coordinated manner, ranging from joint awareness raising and information gathering to enforcement sweeps and joint investigations. The CEF will facilitate the coordination of enforcement actions driven by commonly identified priorities and using common methodologies.
- **Key action 3:** establish a **Support Pool of Experts (SPE)** on the basis of a pilot project, with a view of providing material support in the form of expertise that is useful for investigations and enforcement activities of significant common interest and to enhance the cooperation and solidarity between all SAs by reinforcing and complementing the strengths of the individual SAs and addressing operational needs.

Adopted

4 PILLAR 3: A FUNDAMENTAL RIGHTS APPROACH TO NEW TECHNOLOGIES

7. The protection of personal data helps to ensure that technology, new business models and society develop in accordance with our values, such as human dignity, autonomy and liberty. The EDPB will continuously monitor new and emerging technologies and their potential impact on the fundamental rights and daily lives of individuals. Data protection should work for all people, particularly in the face of processing activities presenting the greatest risks to individuals' rights and freedoms (e.g. to prevent discrimination). We will help to shape Europe's digital future in line with our common values and rules. We will continue to work with other regulators and policymakers to promote regulatory coherence and enhanced protection for individuals.

- **Key Action 1**: **Assessing new technologies:** proactively monitoring, assessing and establishing common positions and guidance as regards new technological applications in areas such as artificial intelligence (AI), biometrics, profiling, ad tech and continuous evaluation of existing positions on applications such as cloud services, blockchain etc.
- **Key Action 2**: **Reinforcing data protection by design and by default and accountability**: provide clear guidance on how to implement data protection principles effectively, what individuals are entitled to expect and what organisations can do to further improve the ability of individuals to exercise control over their personal data and demonstrate compliance with their obligations.
- **Key Action 3**: intensify **engagement and cooperation with other regulators** (e.g. consumer protection and competition authorities) **and policymakers** to ensure that individuals receive optimal protection and to prevent harms from occurring, including where necessary or appropriate in the context of open consultations on new draft proposals or new projects.

5 PILLAR 4: THE GLOBAL DIMENSION

8. The EDPB is determined to set and promote high EU and global standards for international data transfers to third countries in the private and the public sector, including in the law enforcement sector. We will reinforce our engagement with the international community to promote EU data protection as a global model and to ensure effective protection of personal data beyond EU borders.

- **Key Action 1: Promote the use of transfer tools ensuring an essentially equivalent level of protection and increase awareness on their practical implementation**: develop and provide further practical guidance on how these transfer tools – especially new ones - can maintain a high level of protection of personal data transferred from the EEA to third countries, taking into account the risks linked to access to personal data by the public authorities of third countries and the need to ensure enforceable rights, effective redress and safeguards concerning onward transfers.
- **Key Action 2: Engaging with the international community**: the EDPB and its members will strive to engage in dialogue with international organisations and institutional networks in order to provide leadership in data protection and promote high standards of protection worldwide.

Adopted

- **Key Action 3**: facilitate the engagement between EDPB members and the supervisory authorities of third countries with a focus on **cooperation in enforcement cases** involving controllers/processors located outside the EEA.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Adopted

GRUPA ROBOCZA ART. 29

17/PL
WP259 rev.01

Grupa Robocza Art. 29
Wytyczne dotyczące zgody na mocy rozporządzenia 2016/679

Przyjęte dnia 28 listopada 2017 r.
Ostatnio zmienione i przyjęte dnia 10 kwietnia 2018 r.

GRUPA ROBOCZA DS. OCHRONY OSÓB FIZYCZNYCH W ZAKRESIE

PRZETWARZANIA DANYCH OSOBOWYCH

powołana na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r.,

uwzględniając art. 29 i 30 tej dyrektywy,

uwzględniając swój regulamin wewnętrzny,

PRZYJMUJE NINIEJSZE WYTYCZNE:

Grupa Robocza została powołana na mocy art. 29 dyrektywy 95/46/WE. Jest ona niezależnym europejskim organem doradczym w zakresie ochrony danych i prywatności. Zadania Grupy zostały określone w przepisach art. 30 dyrektywy 95/46/WE i art. 15 dyrektywy 2002/58/WE.
Obsługę sekretariatu zapewnia Dyrekcja C (Prawa Podstawowe i Obywatelstwo Unii Europejskiej) Dyrekcji Generalnej ds. Sprawiedliwości Komisji Europejskiej, B-1049 Bruksela, Belgia, biuro MO-59 02/013.
Strona internetowa: http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358&tpa_id=6936

Spis treści

1. Wprowadzenie ... 3
2. Pojęcie zgody zawarte w art. 4 pkt 11 RODO ... 4
3. Elementy ważnej zgody ... 5
3.1. Dobrowolna / dobrowolnie wyrażona ... 5
3.1.1. Brak równowagi sił ... 6
3.1.2. Warunkowość ... 8
3.1.3. Szczegółowość ... 11
3.1.4. Niekorzystne konsekwencje ... 11
3.2. Konkretność ... 12
3.3. Świadoma ... 14
3.3.1. Minimalne wymogi dotyczące treści, aby zgoda była „świadoma" ... 14
3.3.2. W jaki sposób należy przekazywać informacje? ... 15
3.4. Jednoznaczne oświadczenie woli ... 17
4. Uzyskanie wyraźnej zgody ... 20
5. Dodatkowe warunki uzyskania ważnej zgody ... 22
5.1. Wykazanie zgody ... 22
5.2. Wycofanie zgody ... 24
6. Zależność między zgodą a innymi zgodnymi z prawem podstawami, o których mowa w art. 6 RODO . 25
7. Szczególnie istotne obszary w RODO ... 26
7.1. Dzieci (art. 8) ... 26
7.1.1. Usługi społeczeństwa informacyjnego ... 27
7.1.2. Usługi oferowane bezpośrednio dziecku ... 28
7.1.3. Wiek ... 28
7.1.4. Zgoda udzielana przez dzieci i władza rodzicielska ... 29
7.2. Badania naukowe ... 31
7.3. Prawa osób, których dane dotyczą ... 33
8. Zgoda uzyskana na mocy dyrektywy 95/46/WE ... 34

1. Wprowadzenie

Niniejsze wytyczne zawierają szczegółową analizę pojęcia zgody zastosowanego w rozporządzeniu 2016/679, tj. w ogólnym rozporządzeniu o ochronie danych (zwanym dalej „RODO"). Pojęcie zgody stosowane dotychczas w dyrektywie o ochronie danych (zwanej dalej „dyrektywą 95/46/WE") oraz w dyrektywie o prywatności i łączności elektronicznej ewoluowało. W RODO jeszcze bardziej sprecyzowano i uszczegółowiono wymogi dotyczące uzyskania ważnej zgody oraz wykazania jej wyrażenia. W niniejszych wytycznych skoncentrowano się na tych zmianach i sformułowano praktyczne wskazówki w celu zapewnienia zgodności z RODO, opierając się na opinii 15/2011 w sprawie definicji zgody. Na administratorach danych spoczywa obowiązek wprowadzania innowacji w celu znalezienia nowych rozwiązań, które funkcjonują w ramach prawnych i lepiej wspierają ochronę danych osobowych oraz interesy osób, których dane dotyczą.

Zgoda jest jedną z sześciu zgodnych z prawem podstaw przetwarzania danych osobowych wymienionych w art. 6 RODO[1]. Rozpoczynając działalność, która wiąże się z przetwarzaniem danych osobowych, administrator musi zawsze poświęcić pewien czas na zastanowienie się, jaka byłaby odpowiednia zgodna z prawem podstawa planowanego przetwarzania.

Co do zasady zgoda może być właściwą, zgodną z prawem podstawą wyłącznie wówczas, gdy osobie, której dane dotyczą, zapewnia się kontrolę oraz rzeczywistą możliwość wyboru w odniesieniu do przyjęcia lub odrzucenia zaoferowanych warunków lub odrzucenia ich bez niekorzystnych konsekwencji. Zwracając się o zgodę, administrator ma obowiązek oceny, czy spełni wszystkie wymogi uzyskania ważnej zgody. Zgoda uzyskana w pełnej zgodności z RODO jest narzędziem zapewniającym osobom, których dane dotyczą, kontrolę nad tym, czy dotyczące ich dane osobowe będą przetwarzane. W braku zgodności zgody z RODO kontrola ze strony osoby, której dane dotyczą, staje się złudna, a zgoda będzie nieważną podstawą przetwarzania, co spowoduje niezgodność z prawem czynności przetwarzania[2].

Istniejące opinie Grupy Roboczej Art. 29 (GR29) w sprawie zgody[3] nadal mają zastosowanie, jeżeli są zgodne z nowymi ramami prawnymi, ponieważ w RODO skodyfikowano istniejące wytyczne GR29 i ogólne dobre praktyki oraz większość najważniejszych elementów zgody pozostaje jednakowa na mocy RODO. W niniejszym dokumencie GR29 rozszerza i uzupełnia zatem wcześniejsze opinie dotyczące określonych zagadnień, które zawierają odniesienie do zgody na podstawie dyrektywy 95/46/WE, nie zastępując tych opinii.

Jak stwierdzono w opinii 15/2011 w sprawie definicji zgody, zwracanie się do osób o wyrażenie zgody na czynność przetwarzania danych powinno podlegać rygorystycznym wymogom, ponieważ dotyczy praw podstawowych osób, których dane dotyczą, a administrator pragnie przeprowadzić

[1] Art. 9 RODO zawiera wykaz możliwych wyjątków od zakazu przetwarzania szczególnych kategorii danych. Jeden z wymienionych wyjątków dotyczy sytuacji, w której osoba, której dane dotyczą, udzieli wyraźnej zgody na wykorzystanie tych danych.
[2] Zob. również opinia 15/2011 w sprawie definicji zgody (WP 187), s. 6–8 lub opinia 06/2014 w sprawie pojęcia uzasadnionych interesów administratora danych zawartego w art. 7 dyrektywy 95/46/WE (WP 217), s. 9, 10, 13 i 14.
[3] W szczególności opinia 15/2011 w sprawie definicji zgody (WP 187).

operację przetwarzania, która byłaby niezgodna z prawem bez zgody osoby, której dane dotyczą[4]. Kluczową rolę zgody podkreślono w art. 7 i 8 Karty praw podstawowych Unii Europejskiej. Ponadto również uzyskanie zgody nie zwalnia administratora z obowiązków przestrzegania zasad przetwarzania zawartych w RODO, w szczególności w art. 5 RODO, w odniesieniu do rzetelności, konieczności i proporcjonalności oraz jakości danych, ani w żaden sposób nie zmniejsza zakresu tych obowiązków. Nawet gdyby osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie danych osobowych, nie uczyniłoby to legalnym gromadzenia danych, które nie są konieczne w związku z określonym celem przetwarzania, i byłoby ono zasadniczo nieuczciwe[5].

Jednocześnie GR29 jest świadoma przeglądu dyrektywy o prywatności i łączności elektronicznej (2002/58/WE). Pojęcie zgody w projekcie rozporządzenia w sprawie prywatności i łączności elektronicznej pozostaje powiązane z pojęciem zgody w RODO[6]. Organizacje prawdopodobnie będą potrzebowały zgody zgodnie z instrumentem dotyczącym prywatności i łączności elektronicznej w odniesieniu do większości internetowych wiadomości marketingowych lub połączeń marketingowych oraz internetowych metod śledzenia, w tym za pośrednictwem plików cookie, aplikacji lub innego oprogramowania. GR29 przedstawiła już prawodawcy Unii zalecenia i wytyczne w zakresie wniosku dotyczącego rozporządzenia w sprawie prywatności i łączności elektronicznej[7].

W odniesieniu do istniejącej dyrektywy o prywatności i łączności elektronicznej GR29 zauważa, że odesłania do uchylonej dyrektywy 95/46/WE należy traktować jako odesłania do RODO[8]. Zasada ta ma również zastosowanie do odniesień do zgody zawartych w obowiązującej dyrektywie 2002/58/WE, ponieważ rozporządzenie w sprawie prywatności i łączności elektronicznej nie wejdzie (jeszcze) w życie od dnia 25 maja 2018 r. Zgodnie z art. 95 RODO nie nakłada się dodatkowych obowiązków co do przetwarzania w związku ze świadczeniem ogólnodostępnych usług łączności elektronicznej w publicznych sieciach łączności w zakresie, w jakim w dyrektywie o prywatności i łączności elektronicznej nałożono szczegółowe obowiązki mające ten sam cel. GR29 zauważa, że wymogów uzyskania zgody określonych w RODO nie uznaje się za „dodatkowy obowiązek", lecz raczej za warunki wstępne zgodnego z prawem przetwarzania. Określone w RODO przesłanki uzyskania ważnej zgody mają zatem zastosowanie w sytuacjach objętych zakresem stosowania dyrektywy o prywatności i łączności elektronicznej.

2. Pojęcie zgody zawarte w art. 4 pkt 11 RODO

W art. 4 pkt 11 RODO zdefiniowano zgodę jako: „dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych".

[4] Opinia 15/2011, strona dotycząca definicji zgody (WP 187), s. 8.
[5] Zob. również opinia 15/2011 w sprawie definicji zgody (WP 187) oraz art. 5 RODO.
[6] Zgodnie z art. 9 proponowanego rozporządzenia w sprawie prywatności i łączności elektronicznej zastosowanie mają definicja i warunki zgody przewidziane w art. 4 pkt 11 i art. 7 RODO.
[7] Zob. opinia 03/2016 w sprawie oceny i przeglądu dyrektywy o prywatności i łączności elektronicznej (WP 240).
[8] Zob. art. 94 RODO.

Podstawowa koncepcja zgody pozostaje podobna do koncepcji zawartej w dyrektywie 95/46/WE, przy czym zgoda stanowi jedną ze zgodnych z prawem podstaw, na których musi się opierać przetwarzanie danych osobowych, zgodnie z art. 6 RODO[9]. Oprócz zmienionej definicji zawartej w art. 4 pkt 11 RODO zawiera dodatkowe wskazówki w art. 7 oraz w motywach 32, 33, 42 i 43 dotyczące sposobu działania administratora w celu spełnienia głównych elementów wymogu uzyskania zgody.

Ponadto uwzględnienie przepisów szczegółowych i motywów dotyczących wycofania zgody potwierdza, że wyrażenie zgody powinno być decyzją odwracalną i że osobie, której dane dotyczą, przysługuje pewien zakres kontroli.

3. Elementy ważnej zgody

Art. 4 pkt 11 RODO stanowi, że zgoda osoby, której dane dotyczą, oznacza:

- dobrowolne,
- konkretne,
- świadome i
- jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

W poniższych sekcjach przeanalizowano, w jakim zakresie brzmienie art. 4 pkt 11 zobowiązuje administratorów do zmiany zapytań o zgodę / formularzy wyrażenia zgody, aby zapewnić zgodność z RODO[10].

3.1. Dobrowolna / dobrowolnie wyrażona[11]

[9] Zgodę zdefiniowano w dyrektywie 95/46/WE jako „konkretne i świadome, dobrowolne wskazanie przez osobę, której dane dotyczą na to, że wyraża przyzwolenie na przetwarzanie odnoszących się do niej danych osobowych", przy czym zgoda ta musi być „jednoznacznie wyrażona", aby zapewnić legalność przetwarzania danych osobowych (art. 7 lit. a) dyrektywy 95/46/WE). Zob. opinia GR29 15/2011 w sprawie definicji zgody (WP 187), aby zapoznać się z przykładami stosowności zgody jako podstawy zgodnej z prawem. W opinii tej GR29 przedstawiła wytyczne w celu dokonania rozróżnienia między przypadkami, w których zgoda stanowi właściwą, zgodną z prawem podstawę, a przypadkami, w których wystarczające jest powołanie się na przesłankę uzasadnionego interesu (ewentualnie z możliwością wyrażenia sprzeciwu) lub zalecane byłoby nawiązanie stosunku umownego. Zob. również opinia GR29 06/2014, pkt III.1.2, s. 14 i nast. Wyraźna zgoda stanowi również jeden z wyjątków od zakazu przetwarzania szczególnych kategorii danych: zob. art. 9 RODO.
[10] Aby uzyskać wskazówki dotyczące bieżących czynności przetwarzania opartych na zgodzie na mocy dyrektywy 95/46, zob. rozdział 7 niniejszego dokumentu oraz motyw 171 RODO.
[11] W szeregu opinii Grupa Robocza Art. 29 zbadała granice zgody w sytuacjach, w których zgoda nie może być dobrowolnie wyrażona. Dokumenty te obejmują w szczególności: opinię 15/2011 w sprawie definicji zgody (WP 187), dokument roboczy w sprawie przetwarzania danych osobowych dotyczących zdrowia w elektronicznej dokumentacji medycznej (WP 131), opinię 8/2001 w sprawie przetwarzanie danych osobowych w związku z zatrudnieniem (WP 48) oraz drugą opinię 4/2009 dotyczącą przetwarzania danych przez Światową Agencję Antydopingową (WADA) (międzynarodowy standard ochrony prywatności i danych osobowych), odpowiednich przepisów kodeksu WADA oraz innych kwestii dotyczących prywatności w kontekście zwalczania dopingu w sporcie przez WADA i inne (krajowe) organizacje antydopingowe (WP 162).

Przymiot „dobrowolności" zakłada rzeczywistą możliwość dokonania wyboru przez osoby, których dane dotyczą, oraz sprawowania przez nie kontroli. Co do zasady RODO stanowi, że jeżeli osobie, której dane dotyczą, nie przysługuje rzeczywista możliwość wyboru, czuje się ona zmuszona do wyrażenia zgody lub poniesie negatywne konsekwencje w przypadku jej niewyrażenia, zgoda będzie nieważna[12]. Jeżeli wyrażenie zgody stanowi nieodłączną i niepodlegającą negocjacji część warunków, uznaje się, że nie jest ona dobrowolna. W związku z tym wyrażenie zgody nie zostanie uznane za dobrowolne, jeżeli osoba, której dane dotyczą, nie może odmówić ani wycofać zgody bez niekorzystnych konsekwencji[13]. Pojęcie braku równowagi między administratorem a osobą, której dane dotyczą, również uwzględniono w RODO.

Podczas oceny, czy zgodę wyrażono dobrowolnie, należy również uwzględnić szczególną sytuację, w której od wyrażenia zgody uzależnione jest wykonanie umowy lub świadczenie usługi, jak opisano w art. 7 ust. 4. Art. 7 ust. 4 ma charakter katalogu otwartego dzięki zastosowaniu w nim wyrażenia „między innymi", które oznacza, że istnieje również szereg innych sytuacji, które mogą zostać objęte zakresem stosowania tego przepisu. Co do zasady wszelki element niewłaściwej presji lub niewłaściwego wpływu na osobę, której dane dotyczą (mogący się przejawiać na wiele różnych sposobów), uniemożliwiający osobie, której dane dotyczą, swobodne złożenie oświadczenia woli, spowoduje nieważność zgody.

> [Przykład 1]
> Aplikacja mobilna do edytowania zdjęć prosi użytkowników o aktywowanie lokalizacji GPS w celu rozpoczęcia korzystania z jej usług. Aplikacja informuje również użytkowników, że będzie wykorzystywała zgromadzone dane do celów reklamy behawioralnej. Ani geolokalizacja, ani internetowa reklama behawioralna nie są konieczne do świadczenia usługi edytowania zdjęć i wykraczają one poza świadczenie podstawowej usługi. Ponieważ użytkownicy nie mogą korzystać z aplikacji bez wyrażenia zgody na te usługi, nie można uznać zgody za wyrażoną dobrowolnie.

3.1.1. Brak równowagi sił

Motyw 43[14] wyraźnie stanowi, że jest mało prawdopodobne, by **organy publiczne** mogły opierać się na zgodzie na przetwarzanie, ponieważ jeżeli administratorem jest organ publiczny, często istnieje wyraźny brak równowagi w stosunkach między administratorem a osobą, której dane dotyczą. W większości przypadków nie ulega również wątpliwości, że osoba, której dane dotyczą, nie będzie miała realnej alternatywy wobec zaakceptowania (warunków) przetwarzania zaproponowanych przez tego administratora. GR29 twierdzi, że istnieją inne zgodne z prawem podstawy, które są co do zasady właściwsze w przypadku działalności organów publicznych[15].

Bez uszczerbku dla tych ogólnych rozważań możliwość wykorzystania zgody jako zgodnej z prawem podstawy przetwarzania danych przez organy publiczne nie jest całkowicie wykluczona zgodnie z ramami prawnymi RODO. Poniższe przykłady pokazują, że wykorzystanie zgody może być właściwe w pewnych okolicznościach.

> [Przykład 2] Gmina planuje przeprowadzenie robót konserwacyjnych na drogach. Ponieważ roboty drogowe mogą powodować długotrwałe utrudnienia w ruchu, gmina oferuje mieszkańcom możliwość zapisania się na listę dystrybucyjną, aby otrzymywać aktualne informacje na temat postępu robót i oczekiwanych opóźnień. Gmina wyjaśnia, że zapisanie się na listę nie jest obowiązkowe, i zwraca się o wyrażenie zgody na wykorzystanie adresów e-mailowych (wyłącznie) w tym celu. Mieszkańcy, którzy nie wyrażą zgody, nie stracą możliwości korzystania z jakiejkolwiek podstawowej usługi gminy ani możliwości wykonania jakiegokolwiek przysługującego im prawa, a zatem mogą dobrowolnie wyrazić zgodę lub odmówić wyrażenia zgody na wykorzystanie tych danych. Wszystkie informacje na temat robót drogowych będą również dostępne na stronie internetowej gminy.
>
> [Przykład 3] Osoba fizyczna będąca właścicielem gruntu musi uzyskać określone zezwolenia zarówno od gminy, jak i od jednostki samorządu terytorialnego wyższego szczebla, której podlega gmina. Obydwa organy publiczne wymagają dostarczenia tych samych informacji w celu wydania zezwolenia, ale nie mają wzajemnego dostępu do swoich baz danych. Obydwa organy zwracają się zatem o te same informacje dotyczące gruntu, a jego właścicielka przekazuje swoje dane obydwu tym instytucjom. Gmina oraz jednostka samorządu terytorialnego wyższego szczebla zwracają się do właścicielki o wyrażenie zgody na połączenie akt, aby uniknąć powielania procedur i korespondencji. Obydwa organy publiczne zapewniają, że jest to nieobowiązkowe i że wnioski o zezwolenie zostaną rozpatrzone osobno, jeżeli nie wyrazi ona zgody na połączenie danych. Wyrażenie przez właścicielkę zgody na połączenie akt przez organy można uznać za dobrowolne.
>
> [Przykład 4] Szkoła publiczna zwraca się do uczniów o wyrażenie zgody na wykorzystanie ich zdjęć w czasopiśmie szkolnym wydawanym w formie papierowej. W tych sytuacjach uczniowie będą mieli faktyczny wybór, jeśli chodzi o wyrażenie zgody, dopóki nie zostanie im odmówiony dostęp do kształcenia lub usług i dopóki będą mogli odmówić wykorzystania tych zdjęć bez żadnych niekorzystnych konsekwencji[16].

Brak równowagi sił występuje również w związku z **zatrudnieniem**[17]. Biorąc pod uwagę zależność charakteryzującą stosunek między pracodawcą a pracownikiem, nie jest prawdopodobne, by osoba, której dane dotyczą, mogła odmówić pracodawcy zgody na przetwarzanie danych, nie doświadczając obaw lub faktycznego ryzyka poniesienia niekorzystnych konsekwencji w wyniku odmowy. Nie jest prawdopodobne, by pracownik mógł swobodnie odpowiedzieć na wniosek pracodawcy o wyrażenie zgody na przykład na uruchomienie systemów monitorowania, takich jak nadzór kamer w miejscu pracy, lub wypełnienie formularzy oceny, nie odczuwając żadnej presji na wyrażenie zgody[18]. GR29 uznaje zatem, że w przypadku pracodawców problematyczne jest przetwarzanie danych osobowych obecnych lub przyszłych pracowników w oparciu o ich zgodę, ponieważ jest mało prawdopodobne, by została ona udzielona dobrowolnie. W odniesieniu do większości przypadków przetwarzania danych w miejscu pracy zgodną z prawem podstawą nie

[12] Zob. opinia 15/2011 w sprawie definicji zgody (WP 187), s. 12.
[13] Zob. motywy 42, 43 RODO oraz opinia GR29 15/2011 w sprawie definicji zgody przyjęta dnia 13 lipca 2011 r. (WP 187), s. 12.
[14] Motyw 43 RODO stanowi: „Aby zapewnić dobrowolność, zgoda nie powinna stanowić ważnej podstawy prawnej przetwarzania danych osobowych w szczególnej sytuacji, w której istnieje wyraźny brak równowagi między osobą, której dane dotyczą, a administratorem, w szczególności gdy administrator jest organem publicznym i dlatego jest mało prawdopodobne, by w tej konkretnej sytuacji zgodę wyrażono dobrowolnie we wszystkich przypadkach (…)".
[15] Zob. art. 6 RODO, w szczególności jego ust. 1 lit. c) oraz ust. 1 lit. e).
[16] Do celów niniejszego przykładu szkoła publiczna oznacza szkołę sfinansowaną ze środków publicznych lub dowolną placówkę edukacyjną zakwalifikowaną jako organ lub podmiot publiczny na mocy prawa krajowego.
[17] Zob. również art. 88 RODO, w którym podkreślono potrzebę ochrony szczególnych interesów pracowników oraz stworzono możliwość ustanowienia wyjątków w przepisach państwa członkowskiego. Zob. również motyw 155.
[18] Zob. opinia 15/2011 w sprawie definicji zgody (WP 187), s. 12–14, opinia 8/2001 w sprawie przetwarzania danych osobowych w związku z zatrudnieniem (WP 48), rozdział 10, dokument roboczy w sprawie nadzoru komunikacji elektronicznej w miejscu pracy (WP 55), pkt 4.2, oraz opinia w 2/2017 w sprawie przetwarzania danych w miejscu pracy (WP 249), pkt 6.2.

może i nie powinna być zgoda pracowników (art. 6 ust. 1 lit. a)) ze względu na charakter stosunków między pracodawcą a pracownikiem[19].

Nie oznacza to jednak, że pracodawcy nigdy nie mogą powoływać się na zgodę jako zgodną z prawem podstawę przetwarzania. Mogą się zdarzyć sytuacje, w których pracodawca ma możliwość wykazania, że zgody faktycznie udzielono dobrowolnie. Biorąc pod uwagę brak równowagi sił między pracodawcą a jego pracownikami, pracownicy mogą wyrazić dobrowolną zgodę wyłącznie w wyjątkowych okolicznościach, w których fakt wyrażenia lub niewyrażenia przez nich zgody nie pociąga za sobą żadnych negatywnych konsekwencji[20].

> [Przykład 5]
> Ekipa filmowa ma zamiar nagrywać w określonej części biura. Pracodawca zwraca się do wszystkich pracowników siedzących w tej części o wyrażenie zgody na filmowanie, ponieważ ich wizerunek może się pojawić na drugim planie filmu. Osoby, które nie chcą być filmowane, nie ponoszą żadnych negatywnych konsekwencji, lecz na czas filmowania otrzymują w zamian takie same biurka w innym miejscu w budynku.

Brak równowagi sił nie ogranicza się do organów publicznych i pracodawców – może on zaistnieć również w innych sytuacjach. Jak podkreśliła GR29 w szeregu opinii, zgoda może być ważna wyłącznie wówczas, gdy osoba, której dane dotyczą, ma możliwość dokonania rzeczywistego wyboru i nie zachodzi ryzyko wprowadzenia w błąd, zastraszenia, przymusu lub znaczących negatywnych konsekwencji (np. znaczących kosztów dodatkowych), jeżeli nie wyrazi zgody. Zgoda nie będzie dobrowolna wówczas, gdy pojawi się jakikolwiek element przymusi, presji lub braku możliwości swobodnego złożenia oświadczenia woli.

3.1.2. Warunkowość

Podczas oceny, czy zgodę wyrażono dobrowolnie, istotną rolę odgrywa art. 7 ust. 4 RODO[21].

Art. 7 ust. 4 RODO stanowi, że za wysoce niepożądaną uznaje się między innymi sytuację łączenia zgody z akceptacją warunków lub uzależniania wykonania umowy lub świadczenia usługi od uwzględnienia wniosku o wyrażenie zgody na przetwarzanie danych osobowych, które nie jest konieczne w celu wykonania umowy lub świadczenia usługi. Jeżeli zgodę wyrażono w takiej sytuacji, uznaje się, że nie była ona dobrowolna (motyw 43). Art. 7 ust. 4 dąży do zapewnienia, by cel przetwarzania danych osobowych nie był ukryty ani połączony z wykonaniem umowy lub świadczeniem usługi, w odniesieniu do których odnośne dane osobowe nie są konieczne. Tym samym RODO zapewnia, by przetwarzanie danych osobowych, którego dotyczy wniosek o wyrażenie zgody, nie nosiło bezpośrednich ani pośrednich znamion świadczenia wzajemnego związanego z wykonaniem umowy. Nie można łączyć obydwu tych legalnych podstaw zgodnego z prawem przetwarzania danych osobowych, tj. zgody i umowy, ani zacierać różnic między nimi.

[19] Zob. opinia 2/2017 na temat przetwarzania danych w miejscu pracy, s. 6–7.
[20] Zob. również opinia 2/2017 na temat przetwarzania danych w miejscu pracy (WP 249), pkt 6.2.
[21] Art. 7 ust. 4 RODO: „Oceniając, czy zgodę wyrażono dobrowolnie, w jak największym stopniu uwzględnia się, czy między innymi od zgody na przetwarzanie danych nie jest uzależnione wykonanie umowy, w tym świadczenie usługi, jeśli przetwarzanie danych osobowych nie jest niezbędne do wykonania tej umowy". Zob. również motyw 43 RODO, który stanowi: „Zgody nie uważa się za dobrowolną, jeżeli nie można jej wyrazić z osobna na różne operacje przetwarzania danych osobowych, mimo że w danym przypadku byłoby to stosowne, lub jeżeli od zgody uzależnione jest wykonanie umowy – w tym świadczenie usługi – mimo że do jej wykonania zgoda nie jest niezbędna".

Obowiązek wyrażenia zgody na wykorzystanie danych osobowych w sposób wykraczający poza niezbędne minimum ogranicza przysługującą osobie, której dane dotyczą, możliwość wyboru i uniemożliwia wyrażenie dobrowolnej zgody. Ponieważ celem prawa w dziedzinie ochrony danych jest ochrona praw podstawowych, kontrola osoby fizycznej nad jej danymi osobowymi jest kluczowa, przy czym istnieje silne domniemanie, że zgody na przetwarzanie danych osobowych, które nie jest konieczne, nie można postrzegać jako obowiązkowego świadczenia w zamian za wykonanie umowy lub świadczenie usługi.

W związku z powyższym w każdym przypadku, w którym wniosek o wyrażenie zgody jest związany z wykonaniem umowy przez administratora, osoba, której dane dotyczą i która nie chce udostępnić swoich danych osobowych w celu ich przetwarzania przez administratora, ponosi ryzyko odmowy świadczenia usług, o które się zwróciła.

Aby ocenić, czy w danej sytuacji doszło do powiązania zgody z wykonaniem umowy lub do uzależnienia wykonania umowy od wyrażenia zgody, istotne jest ustalenie zakresu umowy oraz danych, jakie byłyby niezbędne do jej wykonania.
Zgodnie z opinią 06/2014 wydaną przez GR29 należy stosować wykładnię zawężającą wyrażenia „niezbędne do wykonania umowy". Przetwarzanie musi być niezbędne do wykonania umowy z każdą konkretną osobą, której dane dotyczą. Może to obejmować na przykład przetwarzanie adresu osoby, której dane dotyczą, żeby można było dostarczyć towary zakupione przez nią w internecie, lub przetwarzanie danych karty kredytowej w celu ułatwienia płatności. W kontekście zatrudnienia podstawa ta może przykładowo umożliwiać przetwarzanie informacji o wynagrodzeniu i danych rachunku bankowego, żeby można było wypłacić wynagrodzenie[22]. Musi istnieć bezpośredni i obiektywny związek między przetwarzaniem danych a celem wykonania umowy.

Jeżeli administrator zamierza przetwarzać dane osobowe, które są faktycznie niezbędne do wykonania umowy, zgoda nie jest właściwą, zgodną z prawem podstawą[23].

Art. 7 ust. 4 ma zastosowanie wyłącznie wówczas, gdy wnioskowane dane **nie** są niezbędne do wykonania umowy (w tym świadczenia usługi), lecz jej wykonanie uzależniono od uzyskania tych danych w oparciu o zgodę. Jeżeli natomiast przetwarzanie **jest** niezbędne do wykonania umowy (w tym świadczenia usługi), art. 7 ust. 4 nie ma zastosowania.

> [Przykład 6]
> Bank prosi klientów o zgodę na wykorzystywanie przez osoby trzecie ich danych płatniczych do celów marketingu bezpośredniego. Tego rodzaju czynność przetwarzania nie jest niezbędna do wykonania umowy z klientem i świadczenia zwykłych usług w zakresie rachunków bankowych. Jeżeli niewyrażenie przez klienta

[22] Aby uzyskać więcej informacji i zapoznać się z przykładami, zob. opinia 06/2014 w sprawie pojęcia uzasadnionych interesów administratora danych zawartego w art. 7 dyrektywy 95/46/WE przyjęta przez GR29 dnia 9 kwietnia 2014 r., s. 16–17 (WP 217).
[23] W takiej sytuacji właściwą, zgodną z prawem podstawą mogłaby być podstawa określona w art. 6 ust. 1 lit. b) (umowa).

zgody na to przetwarzanie doprowadziłoby do odmowy świadczenia usług bankowych, zamknięcia rachunku bankowego lub – w zależności od przypadku – zwiększenia opłaty, nie można uznać zgody za dobrowolną.

Decyzja prawodawcy o podkreśleniu m.in. warunkowości jako domniemania braku dobrowolności zgody, pokazuje, że wystąpienie warunkowości należy dokładnie zbadać. Wyrażenie „w jak największym stopniu" zastosowane w art. 7 ust. 4 sugeruje, że administrator powinien zachować szczególną ostrożność, jeżeli umowa (która obejmuje świadczenie usługi) zawiera wniosek o wyrażenie zgody na przetwarzanie danych osobowych.

Ponieważ art. 7 ust. 4 nie został sformułowany w sposób bezwzględny, może istnieć bardzo ograniczona liczba przypadków, w których taka warunkowość nie spowodowałaby nieważności zgody. Zastosowanie terminu „uważa się" w motywie 43 wyraźnie wskazuje jednak, że jest to możliwe wyłącznie w wyjątkowych przypadkach.

W każdym przypadku ciężar dowodu zgodnie z art. 7 ust. 4 spoczywa na administratorze[24]. Ten przepis szczegółowy odzwierciedla ogólną zasadę rozliczalności, która przewija się w całym RODO. Jeżeli jednak art. 7 ust. 4 ma zastosowanie, administratorowi będzie trudniej udowodnić, że osoba, której dane dotyczą, udzieliła dobrowolnej zgody[25].

Administrator mógłby argumentować, że jego organizacja zapewnia osobom, których dane dotyczą, rzeczywistą możliwość wyboru, jeżeli mogą one wybierać między usługą, która obejmuje wyrażenie zgody na wykorzystywanie ich danych osobowych do celów dodatkowych, z jednej strony, a równoważną usługą oferowaną przez tego samego administratora, która nie obejmuje zgody na wykorzystywanie danych do celów dodatkowych, z drugiej strony. Jeżeli istnieje możliwość wykonania umowy lub świadczenia zleconej usługi przez tego administratora bez konieczności wyrażenia zgody na tego rodzaju inne lub dodatkowe wykorzystanie danych, oznacza to, że usługa nie ma już charakteru warunkowego. Obydwie usługi muszą być jednak faktycznie równoważne.

Zdaniem GR29 zgody nie można uznać za dobrowolną, jeżeli administrator argumentuje, że istnieje możliwość wyboru między usługą, która obejmuje wyrażenie zgody na wykorzystywanie danych osobowych do celów dodatkowych, z jednej strony, a równoważną usługą oferowaną przez innego administratora, która nie obejmuje zgody na wykorzystywanie danych, z drugiej strony. W takim przypadku swoboda wyboru byłaby zależna od działań innych uczestników rynku oraz od tego, czy konkretna osoba, której dane dotyczą, uznałaby usługi świadczone przez drugiego administratora za faktycznie równoważne. Ponadto nakładałoby to na administratorów obowiązek monitorowania rozwoju sytuacji rynkowej, aby zapewnić ciągłą ważność zgody na podejmowane przez nich

[24] Zob. również art. 7 ust. 1 RODO, który stanowi, że administrator musi wykazać, iż zgoda osoby, której dane dotyczą, była dobrowolna.

[25] W pewnym stopniu wprowadzenie tego ustępu stanowi kodyfikację istniejących wytycznych GR29. Jak opisano w opinii 15/2011, jeżeli osoba, której dane dotyczą, znajduje się w sytuacji zależności od administratora danych ze względu na charakter relacji lub szczególne okoliczności, może istnieć silne domniemanie, że w takich sytuacjach dobrowolność zgody jest ograniczona (np. w przypadku stosunku pracy lub gromadzenia danych przez organ publiczny). Jeżeli art. 7 ust. 4 ma zastosowanie, administratorowi będzie trudniej udowodnić, że osoba, której dane dotyczą, udzieliła dobrowolnej zgody. Zob. opinia 15/2011 w sprawie definicji zgody (WP 187), s. 12–17.

czynności przetwarzania danych, ponieważ konkurent może zmienić świadczoną usługę na późniejszym etapie. Zastosowanie tego argumentu oznacza zatem, że zgoda ta jest niezgodna z RODO.

3.1.3. Szczegółowość

Usługa może obejmować wiele operacji przetwarzania w więcej niż jednym celu. W takich przypadkach osobom, których dane dotyczą, powinna przysługiwać swoboda wyboru celu, który akceptują, zamiast obowiązku wyrażenia zgody na szereg celów przetwarzania. W danym przypadku zgodnie z RODO uzasadnione może być wyrażenie kilku zgód w celu rozpoczęcia oferowania usługi.

W motywie 43 wyjaśniono, że zgody nie uważa się za dobrowolną, jeżeli proces/procedura uzyskania zgody uniemożliwia osobom, których dane dotyczą, wyrażenie osobnej zgody odpowiednio na różne operacje przetwarzania danych osobowych (np. wyłącznie na niektóre operacje przetwarzania, z wyłączeniem pozostałych), chociaż w danym przypadku byłoby to w właściwe. Motyw 32 stanowi, że: „[z]goda powinna dotyczyć wszystkich czynności przetwarzania dokonywanych w tym samym celu lub w tych samych celach. Jeżeli przetwarzanie służy różnym celom, potrzebna jest zgoda na wszystkie te cele".

Jeżeli administrator połączył kilka celów przetwarzania i nie zwrócił się o osobną zgodę na każdy z tych celów, osoba, której dane dotyczą, jest pozbawiona swobody wyboru. Wspomniana szczegółowość jest ściśle związana z faktem, że zgoda musi być konkretna, jak omówiono w sekcji 3.2 poniżej. W przypadku przetwarzania danych do kilku celów rozwiązaniem umożliwiającym spełnienie przesłanek ważnej zgody jest szczegółowość, tj. rozdzielenie tych celów i uzyskanie zgody na każdy z nich.

> [Przykład 7]
> W jednym zapytaniu o zgodę sprzedawca detaliczny zwraca się do klientów o wyrażenie zgody na wykorzystywanie ich danych do celów marketingu elektronicznego oraz na udostępnianie tych danych innym przedsiębiorstwom należącym do grupy. Tego rodzaju zgoda nie jest szczegółowa, ponieważ klient nie wyraża osobnej zgody na te dwa odrębne cele, a zatem zgoda jest nieważna. W tym przypadku należy uzyskać konkretną zgodę na przekazanie danych kontaktowych partnerom handlowym. Tego rodzaju konkretna zgoda zostanie uznana za ważną w odniesieniu do każdego z partnerów (zob. również sekcja 3.3.1), o którego tożsamości poinformowano osobę, której dane dotyczą, w chwili wyrażania zgody, o ile zostanie mu ona przekazana w tym samym celu (w niniejszym przykładzie: do celów marketingowych).

3.1.4. Niekorzystne konsekwencje

Administrator musi wykazać możliwość odmówienia lub wycofania zgody bez niekorzystnych konsekwencji (motyw 42). Na przykład administrator musi udowodnić, że wycofanie zgody nie pociąga za sobą żadnych kosztów dla osoby, której dane dotyczą, a zatem nie wiąże się z żadną wyraźną szkodą dla osób wycofujących zgodę.

Inne przykłady niekorzystnych konsekwencji obejmują wprowadzenie w błąd, zastraszanie, przymus lub znaczące negatywne skutki dla osoby, której dane dotyczą i która nie wyraziła zgody. Administrator powinien być w stanie udowodnić, że osobie, której dane dotyczą, przysługiwała

swoboda wyboru lub faktyczna możliwość wyboru co do udzielenia zgody i że miała możliwość wycofania zgody bez niekorzystnych konsekwencji.

Jeżeli administrator może wykazać, że usługa obejmuje możliwość wycofania zgody bez żadnych negatywnych konsekwencji, tj. bez obniżenia jakości usługi na szkodę użytkownika, może to świadczyć o dobrowolnym wyrażeniu zgody. RODO nie wyklucza wszystkich zachęt, jednak ciężar udowodnienia dobrowolnego charakteru zgody we wszystkich okolicznościach spoczywałby na administratorze.

[Przykład 8]
Podczas pobierania lifestylowa aplikacja mobilna prosi o wyrażenie zgody na dostęp do miernika przyspieszenia telefonu. Nie jest to konieczne do funkcjonowania aplikacji, ale użyteczne dla administratora, który chciałby uzyskać więcej informacji na temat przemieszczeń i poziomów aktywności użytkowników aplikacji. W przypadku wycofania zgody przez użytkowniczkę okazuje się, że aplikacja działa obecnie jedynie w ograniczonym zakresie. Jest to przykład niekorzystnych konsekwencji w rozumieniu motywu 42, co oznacza, że zgoda nie została uzyskana w sposób ważny (a zatem administrator musi wykasować wszystkie zgromadzone w ten sposób dane osobowe dotyczące przemieszczeń użytkowników).

[Przykład 9]
Osoba, której dane dotyczą, dokonuje subskrypcji biuletynu detalisty odzieżowego oferującego ogólne zniżki. Detalista zwraca się do osoby, której dane dotyczą, o zgodę na gromadzenie większej ilości danych na temat jej preferencji zakupowych, aby dostosować oferty do jej preferencji na podstawie historii zakupów lub kwestionariusza, którego wypełnienie jest dobrowolne. Jeżeli osoba, której dane dotyczą, wycofa następnie zgodę, otrzyma ponownie niespersonalizowane zniżki odzieżowe. Nie można uznać tego faktu za niekorzystne konsekwencje, ponieważ utracono jedynie dopuszczalną zachętę.

[Przykład 10]
Magazyn o modzie oferuje czytelnikom dostęp do nowych produktów do makijażu przed ich oficjalnym wprowadzeniem na rynek.
Produkty będą wkrótce dostępne w sprzedaży, jednak czytelnicy magazynu mogą uczestniczyć w ekskluzywnej możliwości wypróbowania tych produktów. Aby skorzystać z tej oferty, muszą oni podać swój adres korespondencyjny i wyrazić zgodę na umieszczenie na liście dystrybucyjnej magazynu. Adres korespondencyjny jest niezbędny do wysyłki, natomiast lista dystrybucyjna jest wykorzystywana w celu wysyłania ofert handlowych produktów, takich jak kosmetyki czy koszulki, przez cały rok.
Przedsiębiorstwo wyjaśnia, że dane dostępne na liście dystrybucyjnej będą wykorzystywane wyłącznie do wysyłania towarów i innych reklam w formie papierowej przez sam magazyn i nie zostaną udostępnione żadnej innej organizacji.
Jeżeli czytelnik nie chce ujawnić swojego adresu z tego powodu, nie poniesie żadnych niekorzystnych konsekwencji, ponieważ i tak będzie miał dostęp produktów.

3.2. Konkretność

W art. 6 ust. 1 lit. a) potwierdzono, że osoba, której dane dotyczą, musi wyrazić zgodę „w jednym lub większej liczbie określonych celów" oraz że osobie tej przysługuje możliwość wyboru w odniesieniu do każdego z nich[26]. Wymóg, zgodnie z którym zgoda musi być „konkretna", ma na celu zapewnienie określonego stopnia kontroli sprawowanej przez użytkownika oraz przejrzystości w odniesieniu do osoby, której dane dotyczą. Wymóg ten nie został zmieniony na mocy RODO i pozostaje ściśle powiązany z wymogiem udzielenia „świadomej" zgody. Jednocześnie należy go interpretować zgodnie z wymogiem dotyczącym „szczegółowości" w celu uzyskania „dobrowolnej" zgody[27]. Podsumowując, aby spełnić wymóg „konkretności" zgody, administrator musi pamiętać o:

(i) określeniu celu jako zabezpieczeniu przed zmianą celu;
(ii) szczegółowości w zapytaniach o zgodę; oraz
(iii) wyraźnym oddzieleniu informacji związanych z uzyskaniem zgody na czynności przetwarzania danych od informacji na inne tematy.

Ad. (i): Zgodnie z art. 5 ust. 1 lit. b) RODO uzyskanie ważnej zgody jest zawsze poprzedzone określeniem konkretnego, wyraźnego i prawnie uzasadnionego celu zamierzonej czynności przetwarzania[28]. Konieczność uzyskania konkretnej zgody w połączeniu z pojęciem ograniczenia celu zawartym w art. 5 ust. 1 lit. b) stanowi zabezpieczenie przed stopniowym rozszerzaniem lub zacieraniem celów, w których dane są przetwarzane, po wyrażeniu przez osobę, której dane dotyczą, zgody na pierwotne gromadzenie danych. Zjawisko to, znane również jako zmiana celu, stanowi ryzyko dla osób, których dane dotyczą, ponieważ może prowadzić do niespodziewanego wykorzystania danych osobowych przez administratora lub przez osoby trzecie oraz do utraty kontroli przez osobę, której dane dotyczą.

Jeżeli administrator opiera się na art. 6 ust. 1 lit. a), osoby, których dane dotyczą, muszą zawsze wyrazić zgodę na konkretny cel przetwarzania[29]. Zgodnie z koncepcją *ograniczenia celu* określoną w art. 5 ust. 1 lit. b) i motywie 32 zgoda może obejmować różne operacje, o ile operacje te służą temu samemu celowi. Nie ulega wątpliwości, że konkretną zgodę można uzyskać wyłącznie wówczas, gdy osoby, których dane dotyczą, zostaną konkretnie poinformowane o zamierzonych celach wykorzystywania danych, które ich dotyczą.

Niezależnie od przepisów dotyczących zgodności celów zgoda musi dotyczyć konkretnego celu. Osoby, których dane dotyczą, wyrażą zgodę, zakładając, że sprawują nad nimi kontrolę i że ich dane będą przetwarzane wyłącznie w tych określonych celach. Jeżeli administrator przetwarza dane na podstawie zgody i chciałby przetwarzać dane w nowym celu, musi zwrócić się do osoby, której dane dotyczą, o dodatkową zgodę na ten inny cel, chyba że istnieje inna zgodna z prawem podstawa, która lepiej odzwierciedla sytuację.

[Przykład 11] Sieć telewizji kablowej gromadzi dane osobowe abonentów na podstawie ich zgody, aby przedstawiać im spersonalizowane propozycje nowych filmów, które mogą ich zainteresować, w oparciu o ich upodobania w zakresie oglądanych programów. Po pewnym czasie sieć telewizyjna decyduje, że chciałaby umożliwić osobom trzecim wysyłanie (lub wyświetlanie) reklamy ukierunkowanej na podstawie upodobań abonentów w zakresie oglądanych programów. Zważywszy na nowy cel, potrzebna jest nowa zgoda.

[26] Dalsze wskazówki na temat określania „celów" są dostępne w opinii 3/2013 w sprawie ograniczenia celu (WP 203).

[27] Motyw 43 RODO stanowi, że w stosownych przypadkach konieczne będzie uzyskanie osobnej zgody na różne operacje przetwarzania. Należy zapewnić osobom, których dane dotyczą, możliwość wyrażenia szczegółowej zgody, aby umożliwić im udzielenie osobnej zgody na osobne cele.

[28] Zob. opinia GR29 3/2013 w sprawie ograniczenia celu (WP 203), s. 16: „Z tych powodów cel, który jest niejednoznaczny lub ogólny, taki jak na przykład »poprawa doświadczeń użytkowników«, »cele marketingowe«, »cele bezpieczeństwa informatycznego« lub »przyszłe badania« – bez podania szczegółów – co do zasady nie będzie spełniał kryteriów »konkretności«".

[29] Jest to zgodne z opinią GR29 15/2011 w sprawie definicji zgody (WP 187), np. s. 17.

Ad. (ii): Aby spełnić wymóg „dobrowolności", mechanizmy zgody muszą być nie tylko szczegółowe, ale muszą również posiadać przymiot „konkretności". Oznacza to, że administrator, który prosi o zgodę na przetwarzanie w wielu różnych celach, powinien zapewnić możliwość wyrażenia zgody osobno na każdy z tych celów, aby umożliwić użytkownikom wyrażenie konkretnej zgody na konkretne cele.

Ad. (iii): Ponadto w każdym osobnym zapytaniu o zgodę administratorzy powinni podać szczegółowe informacje na temat danych, które są przetwarzane w każdym z celów, aby uświadomić osobom, których dane dotyczą, skutki poszczególnych wyborów, jakich mogą dokonać. Osoby, których dane dotyczą, mogą zatem wyrazić konkretną zgodę. Kwestia ta pokrywa się z wymogiem, aby administratorzy zapewniali jednoznaczne informacje, jak omówiono w pkt 3.3 poniżej.

3.3. Świadoma

W RODO wzmocniono wymóg, zgodnie z którym zgoda musi być świadoma. Zgodnie z art. 5 RODO wymóg przejrzystości stanowi jedną z podstawowych zasad, ściśle związaną z zasadami rzetelności i zgodności z prawem. Zapewnianie informacji osobom, których dane dotyczą, przed uzyskaniem ich zgody jest niezbędne do umożliwienia im podejmowania świadomych decyzji, zrozumienia, na co wyrażają zgodę, oraz na przykład wykonania przysługującego im prawa wycofania zgody. Jeżeli administrator nie zapewnia dostępnych informacji, kontrola ze strony użytkownika staje się złudna, a zgoda będzie nieważną podstawą przetwarzania.

Konsekwencją niespełnienia wymogów dotyczących świadomej zgody będzie nieważność zgody i możliwość naruszenia przez administratora art. 6 RODO.

3.3.1. Minimalne wymogi dotyczące treści, aby zgoda była „świadoma"

Aby zgoda była świadoma, należy poinformować osobę, której dane dotyczą, o określonych elementach kluczowych w celu dokonania wyboru. W związku z tym GR29 jest zdania, że do uzyskania ważnej zgody wymagane są przynajmniej następujące informacje:

(i) tożsamość administratora; [30]
(ii) cel każdej operacji przetwarzania, dla której prosi się o zgodę[31];
(iii) jakie dane (jaki rodzaj danych) będą gromadzone i wykorzystywane; [32]
(iv) istnienie prawa do wycofania zgody[33];
(v) informacje dotyczące wykorzystywania danych do celów zautomatyzowanego podejmowania decyzji zgodnie z art. 22 ust. 2 lit. c)[34] w stosownych przypadkach; oraz

[30] Zob. również motyw 42 RODO: „[...] Aby wyrażenie zgody było świadome, osoba, której dane dotyczą, powinna znać przynajmniej tożsamość administratora oraz zamierzone cele przetwarzania danych osobowych [...]".
[31] Zob. ponownie motyw 42 RODO.
[32] Zob. również opinia GR29 15/2011 w sprawie definicji zgody (WP 187), s. 19–20.
[33] Zob. art. 7 ust. 3 RODO.
[34] Zob. również wytyczne GR29 w sprawie zautomatyzowanego podejmowania decyzji i profilowania do celów rozporządzenia 2016/679 (WP 251), pkt IV.B, s. 20 i nast.

(vi) dotyczące możliwych zagrożeń związanych z przekazywaniem danych w związku z brakiem decyzji stwierdzającej odpowiedni stopień ochrony oraz odpowiednich zabezpieczeń zgodnie z art. 46[35].

Jeżeli chodzi o ppkt (i) i (iii), GR29 zauważa, że w przypadku gdy na wnioskowanej zgodzie ma się opierać wielu (współ-)administratorów lub gdy dane mają zostać przekazane innym administratorom lub przetwarzane przez innych administratorów, którzy chcą się opierać na pierwotnej zgodzie, wszystkie te organizacje powinny być wymienione. Podmioty przetwarzające nie muszą być wymienione w ramach wymogów dotyczących zgody, chociaż w celu zapewnienia zgodności z art. 13 i 14 RODO administratorzy będą musieli przedstawić pełen wykaz odbiorców lub kategorii odbiorców, w tym podmiotów przetwarzających. Podsumowując, GR29 zauważa, że w zależności od okoliczności i kontekstu sprawy konieczne może być zapewnienie większej ilości informacji, aby umożliwić osobom, których dane dotyczą, rzeczywiste zrozumienie danych operacji przetwarzania.

3.3.2. W jaki sposób należy przekazywać informacje?

W RODO nie określono formy przekazywania informacji ani ich kształtu w celu spełnienia wymogu świadomej zgody. Oznacza to, że ważne informacje mogą być przekazane na różne sposoby, np. w formie pisemnych lub ustnych oświadczeń bądź wiadomości dźwiękowych lub wiadomości wideo. W RODO ustanowiono jednak szereg wymogów dotyczących świadomej zgody, głównie w art. 7 ust. 2 i motywie 32. Prowadzi to do wyższego standardu jasności i dostępności informacji.

Prosząc o zgodę, administratorzy powinni się upewnić, że używają jasnego i prostego języka we wszystkich przypadkach. Oznacza to, że wiadomość powinna być zrozumiała dla przeciętnej osoby, a nie tylko dla prawników. Administratorzy nie mogą stosować długich i trudnych w zrozumieniu informacji o polityce prywatności ani zamieszczać w nich oświadczeń pełnych żargonu prawniczego. Zgoda musi być jednoznaczna i udzielona w sposób pozwalający wyraźnie odróżnić ją od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie. Wymóg ten oznacza co do zasady, że informacje istotne dla podjęcia świadomych decyzji o wyrażeniu lub niewyrażeniu zgody nie mogą być ukryte w ogólnych warunkach[36].

Administrator musi dopilnować, by zgoda została udzielona na podstawie informacji umożliwiających osobom, których dane dotyczą, łatwą identyfikację administratora oraz zrozumienie, na co wyrażają zgodę. Administrator musi jasno opisać cel przetwarzania danych, którego dotyczy zapytanie o zgodę[37].

[35] Zgodnie z art. 49 ust. 1 lit. a) w przypadku zwrócenia się o wyraźną zgodę wymagane są szczegółowe informacje na temat braku zabezpieczeń opisanych w art. 46. Zob. również opinia GR29 15/2011 w sprawie definicji zgody (WP 187), s. 19.
[36] Oświadczenie o wyrażeniu zgody musi być określone jako takie. Sformułowania, takie jak „Wiem, że...", nie spełniają wymogów jasnego języka.
[37] Zob. art. 4 pkt 11 oraz art. 7 ust. 2 RODO.

Inne szczegółowe wskazówki dotyczące dostępności przedstawiono w wytycznych GR29 w sprawie przejrzystości. Jeżeli zgoda ma zostać wyrażona drogą elektroniczną, zapytanie musi być jasne i zwięzłe. Wielowarstwowe i szczegółowe informacje mogą być właściwym sposobem wywiązania się z podwójnego obowiązku obejmującego z jednej strony precyzyjność i kompletność, a z drugiej strony zrozumiałość.

Administrator musi ocenić, jaki rodzaj odbiorców przekazuje swoje dane osobowe jego organizacji. Przykładowo jeżeli wśród grupy odbiorców znajdują się małoletnie osoby, których dane dotyczą, od administratora oczekuje się dopilnowania, by informacje były zrozumiałe dla małoletnich[38]. Po określeniu swoich odbiorców administratorzy muszą ustalić, jakie informacje powinni dostarczyć, a następnie w jaki sposób przedstawią informacje osobom, których dane dotyczą.

Art. 7 ust. 2 odnosi się do uprzednio sformułowanych pisemnych oświadczeń o wyrażeniu zgody, które dotyczą także innych kwestii. Gdy o zgodę prosi się w ramach umowy (na papierze), zapytanie o zgodę powinno się wyraźnie odróżniać od pozostałych kwestii. Jeżeli umowa na papierze obejmuje wiele aspektów niezwiązanych z kwestią zgody na wykorzystanie danych osobowych, kwestia zgody powinna zostać przedstawiona w wyraźnie odróżniający się sposób lub w odrębnym dokumencie. Podobnie, jeżeli o zgodę prosi się drogą elektroniczną, zapytanie o zgodę musi być odrębne i możliwe do odróżnienia – nie może to być po prostu jeden akapit w warunkach, zgodnie z motywem 32[39]. Aby zapewnić dostosowanie do małych ekranów lub sytuacji, w których miejsce na informacje jest ograniczone, w stosownych przypadkach można rozważyć warstwowy sposób przedstawienia informacji, aby uniknąć nadmiernego wpływu na funkcjonalność lub koncepcję produktu.

Administrator, który polega na zgodzie osoby, której dane dotyczą, musi również wywiązać się z odrębnych obowiązków informacyjnych ustanowionych w art. 13 i 14, aby zapewnić zgodność z RODO. W praktyce wywiązanie się z obowiązków informacyjnych i spełnienie wymogu uzyskania świadomej zgody może w wielu przypadkach prowadzić do przyjęcia zintegrowanego podejścia. Niniejszą sekcję sporządzono jednak przy założeniu, że ważna, „świadoma" zgoda może istnieć nawet wówczas, gdy nie wszystkie elementy określone w art. 13 lub 14 zostaną wspomniane w procesie uzyskiwania zgody (punkty te należy oczywiście wskazać w innych miejscach, takich jak informacje o polityce prywatności przedsiębiorstwa). GR29 wydała odrębne wytyczne dotyczące wymogu przejrzystości.

> [Przykład 12]
> Przedsiębiorstwo X jest administratorem, który otrzymał skargi, że nie jest jasne dla osób, których dane dotyczą, na jakie rodzaje wykorzystywania danych są proszeni o zgodę. Przedsiębiorstwo dostrzega potrzebę sprawdzenia, czy informacje zawarte w zapytaniu o zgodę są zrozumiałe dla osób, których dane dotyczą. Przedsiębiorstwo X organizuje dobrowolne panele testowe wśród konkretnych kategorii swoich klientów i przedstawia uczestnikom testów nowe zaktualizowane informacje dotyczące zgody przed ogłoszeniem ich na zewnątrz. Wybór kategorii klientów dokonywany jest zgodnie z zasadą niezależności oraz w oparciu o standardy zapewniające reprezentatywny, bezstronny wynik. Klienci otrzymują kwestionariusz i wskazują, co zrozumieli z przedstawionych informacji oraz w jaki sposób oceniliby je pod względem zrozumiałości i istotności informacji. Administrator kontynuuje testy do czasu, aż uczestnicy stwierdzą, że informacje są zrozumiałe. Przedsiębiorstwo X sporządza sprawozdanie z testu i umożliwia dostęp do niego w przyszłości. Przykład ten pokazuje możliwy sposób wykazania przez przedsiębiorstwo X, że osoby, których dane dotyczą, otrzymywały jasne informacje przed wyrażeniem zgody na przetwarzanie danych osobowych przez przedsiębiorstwo X.

> [Przykład 13]
> Przedsiębiorstwo przetwarza dane na podstawie zgody. Stosuje ono warstwowe informacje o polityce prywatności obejmujące zapytanie o zgodę. Przedsiębiorstwo ujawnia wszystkie podstawowe informacje na temat administratora oraz planowanych czynności przetwarzania danych[40]. Przedsiębiorstwo nie wskazuje jednak w pierwszej warstwie informacji o polityce prywatności, w jaki sposób można się skontaktować z jego inspektorem ochrony danych. Aby mieć ważną, zgodną z prawem podstawę w rozumieniu art. 6, administrator ten uzyskał ważną „świadomą" zgodę, nawet jeśli dane kontaktowe inspektora ochrony danych nie zostały przekazane osobie, której dane dotyczą, (w pierwszej warstwie informacji) zgodnie z art. 13 ust. 1 lit. b) lub art. 14 ust. 1 lit. b) RODO.

3.4. Jednoznaczne oświadczenie woli

Z RODO wyraźnie wynika, że zgoda wymaga oświadczenia osoby, której dane dotyczą, lub wyraźnego działania potwierdzającego, co oznacza, że musi być zawsze udzielona przez aktywne działanie lub oświadczenie. Musi być oczywiste, że osoba, której dane dotyczą, zgodziła się na określone przetwarzanie.

W art. 2 lit. h) dyrektywy 95/46/WE opisano zgodę jako „wskazanie przez osobę, której dane dotyczą na to, że wyraża przyzwolenie na przetwarzanie odnoszących się do niej danych osobowych". Opierając się na tej definicji, w art. 4 pkt 11 RODO wyjaśniono, że ważna zgoda wymaga *jednoznacznego* oświadczenia woli *w formie oświadczenia lub wyraźnego działania potwierdzającego* zgodnie z poprzednimi wytycznymi wydanymi przez GR29.

„Wyraźne działanie potwierdzające" oznacza, że osoba, której dane dotyczą, musiała podjąć celowe działanie, aby wyrazić zgodę na określone przetwarzanie[41]. Motyw 32 zawiera dodatkowe

[38] Zob. również motyw 58 dotyczący informacji zrozumiałych dla dzieci.

[39] Zob. również motyw 42 i dyrektywa 93/13/WE, w szczególności jej art. 5 (prosty i zrozumiały język, interpretacja wszelkich wątpliwości na korzyść konsumenta) oraz art. 6 (nieważność nieuczciwych postanowień umownych, umowa będzie nadal obowiązywała bez tych postanowień wyłącznie wówczas, gdy będzie to zasadne, w przeciwnym razie cała umowa będzie nieważna).

[40] Należy zauważyć, że gdy tożsamość administratora lub cel przetwarzania danych nie wynikają z pierwszej warstwy informacyjnej warstwowych informacji o polityce prywatności (i znajdują się w kolejnych warstwach), administratorowi danych trudno będzie wykazać, że osoba, której dane dotyczą, udzieliła świadomej zgody, chyba że administrator danych jest w stanie wykazać, iż osoba ta uzyskała dostęp do tych informacji przed udzieleniem zgody.

[41] Zob. dokument roboczy służb Komisji, ocena skutków, załącznik 2, s. 20, jak również s. 105–106: „Jak również wskazano w przyjętej przez GR29 opinii w sprawie zgody, kluczowe wydaje się wyjaśnienie, że ważna zgoda wymaga zastosowania mechanizmów, które nie pozostawiają wątpliwości co do woli wyrażenia zgody przez osobę, której dane dotyczą, przy jednoczesnym spreczyzowaniu, że – w kontekście otoczenia elektronicznego – wykorzystanie domyślnych ustawień, które osoba, której dane dotyczą, musi zmodyfikować, aby odmówić przetwarzania („zgoda oparta na milczeniu"), nie stanowi samo w sobie jednoznacznej zgody. Zapewniłoby to poszczególnym osobom większą kontrolę nad ich własnymi danymi, niezależnie od tego, czy przetwarzanie opiera się na ich zgodzie. Jeżeli chodzi o administratorów danych, nie miałoby to na nich większego wpływu, ponieważ chodzi wyłącznie o wyjaśnienie i lepsze wysłowienie skutków obowiązującej dyrektywy w odniesieniu do przesłanek ważnej i znaczącej zgody uzyskanej od osoby, której dane dotyczą. W szczególności w zakresie, w jakim pojęcie „wyraźnej" zgody precyzowałoby – przez zastąpienie określenia „jednoznaczna" – warunki i jakość zgody oraz nie miałoby na celu rozszerzenia zakresu przypadków i sytuacji, w których należy wykorzystać (wyraźną) zgodę jako podstawę przetwarzania, nie oczekuje się, aby wpływ tego środka na administratorów danych był znaczny".

wskazówki w tym zakresie. Zgodę można uzyskać w formie pisemnego lub (zarejestrowanego) ustnego oświadczenia, w tym drogą elektroniczną.

Być może najbardziej dosłownym sposobem spełnienia kryterium „pisemnego oświadczenia" jest zapewnienie, by osoba, której dane dotyczą, wysłała pismo lub wiadomość e-mail do administratora, wyjaśniając, na co dokładnie się zgadza. Często jest to jednak nierealne. Oświadczenia pisemne mogą przybierać różne formy i rozmiary, które mogłyby być zgodne z RODO.

Bez uszczerbku dla istniejącego (krajowego) prawa umów zgodę można uzyskać w formie zarejestrowanego oświadczenia ustnego, chociaż przed wyrażeniem zgody należy właściwie uwzględnić informacje dostępne dla osoby, której dane dotyczą. Zastosowanie wcześniej zaznaczonych pól ze zgodą jest nieważne na mocy RODO. Milczenie lub bezczynność po stronie osoby, której dane dotyczą, jak również po prostu kontynuowanie korzystania z usługi nie mogą zostać uznane za aktywne wskazanie wyboru.

> [Przykład 14]
> Przy instalowaniu oprogramowania aplikacja prosi osobę, której dane dotyczą, o zgodę na stosowanie niezanonimizowanych raportów o awarii w celu usprawnienia oprogramowania. Zapytaniu o zgodę towarzyszą warstwowe informacje o polityce prywatności zawierające niezbędne wyjaśnienia. Zaznaczając opcjonalne pole o treści „Wyrażam zgodę", użytkownik jest w stanie dokonać ważnego „wyraźnego działania potwierdzającego" w celu wyrażenia zgody na przetwarzanie.

Administrator musi również mieć świadomość, że zgody nie można uzyskać w drodze tej samej czynności co zawarcie umowy czy zaakceptowanie ogólnych warunków usługi. Zbiorczego zaakceptowania ogólnych warunków nie można uznać za wyraźne działanie potwierdzające wyrażenie zgody na wykorzystanie danych osobowych. RODO nie dopuszcza możliwości stosowania przez administratorów wcześniej zaznaczonych pól ani mechanizmów *opt-out* (możliwość rezygnacji), które wymagają ingerencji ze strony osoby, której dane dotyczą, w celu uniemożliwienia zawarcia umowy (na przykład pola *opt-out*)[42].

Jeżeli zgoda ma zostać wyrażona w odpowiedzi na elektroniczne zapytanie o zgodę, zapytanie takie nie powinno zakłócać *niepotrzebnie* korzystania z usługi, której dotyczy[43]. Dokonana w czynny sposób czynność potwierdzająca, za pośrednictwem której osoba, której dane dotyczą, wyraża zgodę, może być konieczna, jeżeli mniej inwazyjny lub zakłócający sposób powodowałby niejednoznaczność. Konieczne może być zatem, aby zapytanie o zgodę zakłóciło w pewnym stopniu korzystanie z usługi w celu zapewnienia skuteczności zapytania.

Zgodnie z wymogami RODO administratorzy mają jednak swobodę w zakresie opracowania procedury wyrażania zgody odpowiedniej dla ich organizacji. W tym zakresie fizyczne działania można zakwalifikować jako wyraźne działania potwierdzające zgodnie z RODO.

[42] Zob. art. 7 ust. 2. Zob. również dokument roboczy 02/2013 dotyczący pozyskiwania zgody na korzystanie z plików cookie (WP 208), s. 3–6.
[43] Zob. motyw 32 RODO.

Administratorzy powinni opracować mechanizmy zgody w sposób, który jest jednoznaczny dla osób, których dane dotyczą. Administratorzy muszą unikać niejednoznaczności i zapewnić, by czynność, za pośrednictwem której udzielana jest zgoda, można było odróżnić od innych czynności. W związku z tym samo kontynuowanie zwykłego korzystania ze strony internetowej nie jest zachowaniem, na podstawie którego można wywnioskować złożenie przez osobę, której dane dotyczą, oświadczenia woli polegającego na wyrażeniu zgody na proponowaną operację przetwarzania.

> [Przykład 15]
> Przesunięcie paska na ekranie, machnięcie przed inteligentną kamerą, obrócenie smartfona zgodnie z ruchem wskazówek zegara lub zakreślenie ósemki mogą być wariantami wyrażenia zgody, o ile zapewnione są jasne informacje i nie ulega wątpliwości, że dany ruch oznacza zgodę w odpowiedzi na konkretne zapytanie (np. przesunięcie paska w lewo oznacza zgodę na wykorzystanie informacji X w celu Y. Należy powtórzyć ruch w celu potwierdzenia). Administrator musi być w stanie wykazać, że zgodę uzyskano w ten sposób, a osoby, których dane dotyczą, muszą mieć możliwość wycofania zgody tak łatwo, jak jej udzieliły.

> [Przykład 16]
> Przewijanie w dół lub przeglądanie strony internetowej nie spełnia wymogu wyraźnego i potwierdzającego działania. Wynika to z faktu, że ostrzeżenie informujące, iż kontynuowanie przewijania zostanie uznane za zgodę, może być trudne do odróżnienia i może zostać przeoczone, jeżeli osoba, której dane dotyczą, szybko przewija duże ilości tekstu, a ponadto takie działanie nie jest wystarczająco jednoznaczne.

W kontekście cyfrowym wiele usług potrzebuje do funkcjonowania danych osobowych, w związku z czym osoby, których dane dotyczą, codziennie otrzymują wiele zapytań o zgodę, na które odpowiada się kliknięciem i przesunięciem. Może to doprowadzić do zmęczenia klikaniem: gdy ma się z nim do czynienia zbyt często, zmniejsza się ich faktyczny skutek ostrzeżenia.

Prowadzi to do sytuacji, w której zapytania o zgodę nie są już czytane. Stanowi to szczególne ryzyko dla osób, których dane dotyczą, ponieważ zazwyczaj zapytania o zgodę dotyczą działań, które są co do zasady niezgodne z prawem w przypadku braku zgody. W RODO nałożono na administratorów obowiązek opracowania sposobów radzenia sobie z tą kwestią.

Często wymienianym przykładem, jak to zrobić w kontekście internetowym, jest uzyskanie zgody użytkowników internetu za pośrednictwem ich ustawień przeglądarki. Takie ustawienia powinny być opracowane zgodnie z przesłankami ważnej zgody określonymi w RODO, takimi jak na przykład fakt, że zgoda powinna być szczegółowa dla każdego z zamierzonych celów oraz że informacje, które mają być przekazane, powinny obejmować informacje o administratorach.

W każdym przypadku zgodę należy bezwzględnie uzyskać przed rozpoczęciem przez administratora przetwarzania danych osobowych, na które potrzebna jest zgoda. GR29 konsekwentnie utrzymywała w poprzednich opiniach, że zgoda powinna być wyrażona przed rozpoczęciem przetwarzania[44]. Chociaż w art. 4 pkt 11 RODO nie przewidziano wyraźnie, że zgoda

[44] GR29 konsekwentnie podtrzymuje to stanowisko od czasu wydania opinii 15/2011 w sprawie definicji zgody (WP 187), s. 30–31.

musi być wyrażona przed rozpoczęciem przetwarzania, jest to jasno dane do zrozumienia. Nagłówek art. 6 ust. 1 oraz sformułowanie „wyraziła" w art. 6 ust. 1 lit. a) wspierają tę interpretację. Z art. 6 oraz motywu 40 wynika logicznie, że ważna, zgodna z prawem podstawa musi istnieć przed rozpoczęciem przetwarzania danych. W związku z tym zgoda powinna być wyrażona przed rozpoczęciem przetwarzania. Co do zasady wystarczające może być jednokrotne zapytanie o zgodę osoby, której dane dotyczą. Administratorzy muszą jednak uzyskać nową i konkretną zgodę, jeżeli cele przetwarzania danych zmienią się po uzyskaniu zgody lub jeżeli planowany jest dodatkowy cel przetwarzania.

4. Uzyskanie wyraźnej zgody

Wyraźna zgoda jest wymagana w określonych sytuacjach, gdy pojawia się poważne ryzyko związane z ochroną danych, a zatem w sytuacjach, w których za właściwy uznaje się wysoki poziom indywidualnej kontroli nad danymi osobowymi. Zgodnie z RODO wyraźna zgoda odgrywa istotną rolę w przetwarzaniu szczególnych kategorii danych zgodnie z art. 9, przekazywaniu danych do państw trzecich i organizacji międzynarodowych w przypadku braku odpowiednich zabezpieczeń w art. 49[45] oraz w art. 22 dotyczącym zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach, w tym profilowania[46].

Zgodnie z RODO „oświadczenie lub wyraźne działanie potwierdzające" stanowią warunek wstępny „zwykłej" zgody. Ponieważ wymóg dotyczący „zwykłej" zgody określony w RODO został już podniesiony do wyższego standardu w porównaniu z wymogiem dotyczącym zgody określonym w dyrektywie 95/46/WE, należy wyjaśnić, jakie dodatkowe starania powinien podjąć administrator, aby uzyskać *wyraźną* zgodę od osoby, której dane dotyczą, zgodnie z RODO.

Termin „wyraźna" odnosi się do sposobu wyrażenia zgody przez osobę, której dane dotyczą. Oznacza to, że osoba, której dane dotyczą, musi złożyć w sposób wyraźny oświadczenie o wyrażeniu zgody. Oczywistym sposobem zapewnienia, aby zgoda była wyraźna, byłoby jej wyraźne potwierdzenie w pisemnym oświadczeniu. W stosownych przypadkach administrator mógłby zapewnić podpisanie pisemnego oświadczenia przez osobę, której dane dotyczą, aby rozwiać wszelkie możliwe wątpliwości i zapobiec możliwemu brakowi dowodów w przyszłości[47].

[45] Zgodnie z art. 49 ust. 1 lit. a) RODO wyraźna zgoda może spowodować uchylenie zakazu przekazywania danych do krajów, których prawo w dziedzinie ochrony danych nie zapewnia odpowiedniego stopnia ochrony. Zob. również dokument roboczy w sprawie wspólnej wykładni art. 26 ust. 1 dyrektywy 95/46/WE z dnia 24 października 1995 r. (WP 114), s. 11, w którym GR29 wskazała, że zgoda na przekazywanie danych, które odbywa się okresowo lub stale, nie jest właściwa.

[46] W art. 22 RODO wprowadzono przepisy chroniące osoby, których dane dotyczą, przed podejmowaniem decyzji opartym wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu. Podejmowanie decyzji na tej podstawie jest dozwolone pod określonymi prawnymi warunkami prawnymi. Zgoda odgrywa kluczową rolę w tym mechanizmie ochrony, ponieważ w art. 22 ust. 2 lit. c) RODO wyjaśniono, że administrator może skorzystać z zautomatyzowanego podejmowania decyzji, w tym profilowania, które może istotnie wpływać na daną osobę, w przypadku udzielenia wyraźnej zgody przez osobę, której dane dotyczą. GR29 przygotowała odrębne wytyczne na ten temat: wytyczne GR29 w sprawie zautomatyzowanego podejmowania decyzji i profilowania do celów rozporządzenia 2016/679, 3 października 2017 r. (WP 251).

[47] Zob. również opinia GR29 15/2011 w sprawie definicji zgody (WP 187), s. 25.

Takie podpisane oświadczenie nie jest jednak jedynym sposobem uzyskania wyraźnej zgody i nie można stwierdzić, iż w RODO przewidziano obowiązek uzyskania pisemnych i podpisanych oświadczeń we wszystkich okolicznościach, w których wymagane jest uzyskanie ważnej wyraźnej zgody. Na przykład w kontekście cyfrowym lub online osoba, której dane dotyczą, może być w stanie złożyć wymagane oświadczenie przez wypełnienie formularza elektronicznego, wysłanie wiadomości e-mail, przesłanie zeskanowanego dokumentu opatrzonego podpisem osoby, której dane dotyczą, lub złożenie podpisu elektronicznego. W teorii wykorzystanie oświadczeń ustnych również może zostać uznane za wystarczająco wyraźny sposób uzyskania ważnej wyraźnej zgody, jednak administratorowi może być trudno udowodnić, że spełniono wszystkie przesłanki ważnej wyraźnej zgody w chwili, gdy przyjmowano oświadczenie.

Organizacja może również uzyskać wyraźną zgodę podczas rozmowy telefonicznej, pod warunkiem że informacje dotyczące wyboru są uczciwe, zrozumiałe i jasne i że organizacja zwraca się do osoby, której dane dotyczą, o konkretne potwierdzenie (np. naciśnięcie przycisku lub ustne potwierdzenie).

> [Przykład 17] Administrator danych może również uzyskać wyraźną zgodę od odwiedzającego stronę internetową przez wprowadzenie ekranu umożliwiającego wyrażenie wyraźnej zgody zawierającego pola wyboru „Tak" i „Nie", na przykład „Niniejszym wyrażam zgodę na przetwarzanie moich danych", a nie na przykład „Rozumiem, że moje dane będą przetwarzane". Nie ulega wątpliwości, że należy spełnić przesłanki dotyczące świadomej zgody, jak również pozostałe przesłanki uzyskania ważnej zgody.

> [Przykład 18] Klinika chirurgii plastycznej prosi o wyraźną zgodę do pacjenta na przekazanie jego dokumentacji medycznej ekspertowi, do którego klinika zwraca się o drugą opinię na temat stanu pacjenta. Dokumentacja medyczna jest w formie pliku cyfrowego. Z uwagi na szczególny charakter tych informacji klinika prosi o podpis elektroniczny osobę, której dane dotyczą, w celu uzyskania ważnej wyraźnej zgody oraz aby móc wykazać, że uzyskano wyraźną zgodę[48].

Innym sposobem upewnienia się, że wyraźna zgoda jest ważna, jest dwuetapowa weryfikacja zgody. Na przykład osoba, której dane dotyczą, otrzymuje wiadomość e-mail z zawiadomieniem o tym, że administrator danych zamierza przetwarzać rejestr zawierający dane medyczne. Administrator wyjaśnia w wiadomości e-mail, że prosi o zgodę na wykorzystanie określonego zestawu informacji w konkretnym celu. Jeżeli osoba, której dane dotyczą, zgadza się na wykorzystanie tych danych, administrator prosi ją o odpowiedź w formie wiadomości e-mail zawierającej oświadczenie „Wyrażam zgodę". Po wysłaniu odpowiedzi osoba, której dane dotyczą, otrzymuje link weryfikacyjny, który należy kliknąć, lub wiadomość SMS z kodem weryfikacyjnym w celu potwierdzenia zgody.

W art. 9 ust. 2 nie przewidziano, by charakter danych „niezbędnych do wykonania umowy" był wyjątkiem od ogólnego zakazu przetwarzania szczególnych kategorii danych. W związku z tym administratorzy i państwa członkowskie, które znajdują się w takiej sytuacji, powinni zbadać konkretne wyjątki przewidziane w art. 9 ust. 2 lit. b)–j). Jeżeli żaden z wyjątków przewidzianych w przepisach lit. b)–j) nie będzie miał zastosowania, jedynym możliwym wyjątkiem, który można

[48] Przykład ten pozostaje bez uszczerbku dla rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym.

zastosować zgodnie z prawem do przetwarzania takich danych, jest uzyskanie wyraźniej zgody zgodnie z przewidzianymi w RODO warunkami uzyskania ważnej zgody.

[Przykład 19]
Przedsiębiorstwo lotnicze Holiday Airways oferuje usługę podróżowania z asystą dla pasażerów, którzy np. ze względu na niepełnosprawność nie mogą podróżować bez asysty. Klientka rezerwuje lot z Amsterdamu do Budapesztu i zwraca się o asystę w podróży, aby móc wejść na pokład samolotu. Holiday Airways prosi klientkę o podanie informacji na temat jej stanu zdrowia, aby móc zorganizować dla niej właściwe usługi (istnieje bowiem wiele możliwości, np. podstawienie wózka inwalidzkiego przy bramce do odlotu lub zapewnienie asystenta, który odbędzie z nią podróż od punktu A do punktu B). Holiday Airways prosi o wyraźną zgodę na przetwarzanie danych dotyczących zdrowia tej klientki do celów zorganizowania żądanej usługi asysty w podróży. Dane przetwarzane na podstawie zgody powinny być niezbędne do realizacji żądanej usługi. Ponadto z lotów do Budapesztu można korzystać bez asysty w podróży. Należy zwrócić uwagę, że ponieważ dane są niezbędne do zapewnienia żądanej usługi, przepisy art. 7 ust. 4 nie mają zastosowania.

[Przykład 20]
Dobrze prosperujące przedsiębiorstwo specjalizuje się w produkcji gogli narciarskich i snowboardowych na zamówienia oraz innych rodzajów spersonalizowanych okularów do uprawiania sportu na świeżym powietrzu. Założeniem jest możliwość korzystania z tych produktów bez konieczności noszenia własnych okularów. Przedsiębiorstwo zbiera zamówienia w swoim punkcie centralnym i dostarcza produkty z jednego miejsca do wszystkich krajów w UE. Aby móc dostarczać spersonalizowane produkty klientom z krótkowzrocznością, ten administrator danych prosi o zgodę na wykorzystywanie informacji na temat stanu wzroku klientów. Klienci przekazują przez internet niezbędne dane dotyczące zdrowia, np. swoje dane z recepty, w momencie składania zamówienia. Bez tych danych dostarczenie zamówionych spersonalizowanych okularów nie byłoby możliwe. Przedsiębiorstwo oferuje również kolekcje gotowych gogli korekcyjnych. Klienci, którzy nie chcą udostępniać swoich danych dotyczących zdrowia, mogą skorzystać z wersji gotowych. A zatem wymagana jest wyraźna zgoda zgodnie z art. 9 i zgodę można uznać za dobrowolną.

5. Dodatkowe warunki uzyskania ważnej zgody

W RODO wprowadzono wymogi zapewnienia przez administratorów dodatkowych rozwiązań, aby mogli oni otrzymać i zachować ważną zgodę oraz wykazać jej posiadanie. W art. 7 RODO określono te dodatkowe warunki uzyskania ważnej zgody, w tym przepisy szczegółowe dotyczące przechowywania rejestrów zgód i prawa do łatwego wycofania zgody. Art. 7 stosuje się również do zgód, o których mowa w innych artykułach RODO, np. w art. 8 i 9. Poniżej przedstawiono wskazówki dotyczące dodatkowego wymogu, jakim jest wykazanie ważnej zgody, oraz wycofania zgody.

5.1. Wykazanie zgody

W art. 7 ust. 1 RODO jasno wskazano wyraźny obowiązek wykazania przez administratora, że osoba, której dane dotyczą, wyraziła zgodę. Zgodnie z art. 7 ust. 1 ciężar dowodu spoczywa na administratorze.

Motyw 42 stanowi, że: „jeśli przetwarzanie odbywa się na podstawie zgody osoby, której dane dotyczą, administrator powinien być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na operację przetwarzania".

Administratorzy mogą swobodnie opracowywać metody zapewnienia zgodności z tym przepisem w sposób, który jest spójny z ich bieżącą działalnością. Równocześnie obowiązek wykazania, że administrator uzyskał ważną zgodę, nie powinien sam w sobie prowadzić do nadmiernego przetwarzania dodatkowych danych. Oznacza to, że administratorzy powinni mieć wystarczająco dużo danych, aby móc wykazać związek z przetwarzaniem (aby wykazać, że uzyskano zgodę), ale nie powinni zbierać więcej informacji niż to konieczne.

Do administratora należy udowodnienie, że osoba, której dane dotyczą, wyraziła ważną zgodę. W RODO nie określono dokładnie, w jaki sposób należy to zrobić. Administrator musi być jednak w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę w danym przypadku. Dopóki dane są przetwarzane, dopóty istnieje obowiązek wykazania prawidłowo wyrażonej zgody. Po zakończeniu czynności przetwarzania dowód na wyrażenie zgody nie powinien być przechowywany dłużej niż jest to bezwzględnie konieczne do wywiązania się z prawnego obowiązku lub do ustalenia, dochodzenia lub obrony roszczeń zgodnie z art. 17 ust. 3 lit. b) i e).

Na przykład administrator może prowadzić rejestr uzyskanych oświadczeń o wyrażeniu zgody, tak aby mógł wykazać, w jaki sposób i kiedy uzyskano zgodę oraz jakie informacje przekazano osobie, której dane dotyczą, w momencie uzyskania zgody. Administrator musi być również w stanie wykazać, że osoba, której dane dotyczą, została poinformowana, a procedura zastosowana przez administratora spełniała wszystkie właściwe kryteria uzyskania ważnej zgody. Argumentem za takim wymogiem w przepisach RODO jest fakt, że to administrator jest odpowiedzialny za uzyskanie ważnej zgody od osób, które dane dotyczą, i wdrożone mechanizmy zgody. Przykładowo w kontekście internetowym administrator mógłby przechowywać informacje na temat sesji, w ramach której udzielono zgodę, wraz z dokumentacją obiegu zgody w czasie tej sesji, jak również kopię informacji przedstawionych wówczas osobie, której dane dotyczą. Niewystarczające byłoby natomiast jedynie odniesienie się do prawidłowej konfiguracji strony internetowej.

[Przykład 21] Szpital organizuje program badań naukowych pod nazwą „projekt X", do którego realizacji niezbędna jest dokumentacja dentystyczna prawdziwych pacjentów. Uczestników rekrutuje się telefonicznie spośród pacjentów, którzy dobrowolnie zgodzili się na wpisanie ich na listę kandydatów, do których można się zwrócić w tym celu. Administrator prosi osoby, których dane dotyczą, o wyraźną zgodę na wykorzystanie ich dokumentacji dentystycznej. Zgoda zostaje uzyskana w trakcie rozmowy telefonicznej przez nagranie ustnego oświadczenia osoby, której dane dotyczą, w którym osoba ta potwierdza, że zgadza się na wykorzystanie swoich danych do celów projektu X.

W RODO nie określono ram czasowych, w których taka zgoda jest ważna. Okres ważności zgody zależy od kontekstu, zakresu pierwotnej zgody i oczekiwań osoby, której dane dotyczą. Jeżeli operacje przetwarzania zmienią się lub ewoluują w sposób znaczący, wówczas pierwotna zgoda nie będzie już ważna. W takim wypadku należy uzyskać nową zgodę.

Jako najlepszą praktykę GR29 zaleca, by zgoda była aktualizowana we właściwych odstępach czasu. Ponowne przekazanie wszystkich informacji pomaga zapewnić, by osoba, której dane

dotyczą, w dalszym ciągu była dobrze poinformowana, w jaki sposób wykorzystywane są jej dane i jak może korzystać ze swoich praw[49].

5.2. Wycofanie zgody

Wycofanie zgody zajmuje ważne miejsce w RODO. Przepisy i motywy RODO dotyczące wycofania zgody można uznać za kodyfikację dotychczasowej interpretacji tej kwestii przedstawionej w opiniach GR29[50].

Zgodnie z art. 7 ust. 3 RODO administrator musi zapewnić, by osoba, której dane dotyczą, mogła wycofać zgodę z taką samą łatwością, z jaką jej udzieliła, i w dowolnym momencie. W RODO nie stwierdzono, że udzielanie i cofnięcie zgody musi zawsze odbywać się w ten sam sposób.

Jeżeli jednak w praktyce zgody udziela się drogą elektroniczną przez jedno kliknięcie myszą, przesunięcie lub kliknięcie klawisza, osoby, których dane dotyczą, muszą mieć możliwość wycofania tej zgody w równie łatwy sposób. W przypadku gdy zgoda jest uzyskiwana za pomocą interfejsu użytkownika odrębnego dla danej usługi (np. poprzez stronę internetową, aplikację, konto logowania, interfejs urządzenia IoT lub pocztę elektroniczną), nie ulega wątpliwości, że osoba, której dane dotyczą, musi być w stanie wycofać zgodę poprzez ten sam interfejs elektroniczny, ponieważ przełączenie się na inny interfejs wyłącznie w celu wycofania zgody wymagałoby zbędnego wysiłku. Ponadto osoba, której dane dotyczą, powinna być w stanie wycofać zgodę bez ponoszenia niekorzystnych konsekwencji. Oznacza to m.in. że administrator musi zapewnić, by wycofanie zgody było bezpłatne lub nie pociągało za sobą obniżenia poziomu usług[51].

> [Przykład 22] Festiwal muzyczny sprzedaje bilety za pośrednictwem platformy sprzedaży biletów online. Każdej sprzedaży biletów online towarzyszy zapytanie o zgodę na wykorzystanie danych kontaktowych w celach marketingowych. Aby wyrazić zgodę w tym celu, klienci mogą wybrać „Nie" lub „Tak". Administrator informuje klientów o możliwości wycofania zgody. W tym celu klienci mogą bezpłatnie skontaktować się z centrum obsługi telefonicznej w dniach roboczych w godzinach 8.00–17.00. W tym przykładzie administrator nie spełnił wymogów art. 7 ust. 3 RODO. W tym przypadku wycofanie zgody wymaga połączenia telefonicznego w godzinach pracy, co jest bardziej uciążliwe niż jedno kliknięciem myszą potrzebne do wyrażenia zgody za pośrednictwem platformy sprzedaży biletów online, dostępnej 24 godziny na dobę.

Wymóg łatwego wycofania zgody został opisany w RODO jako niezbędny aspekt ważnej zgody. Jeżeli prawo do wycofania zgody nie spełnia wymogów RODO, wówczas stosowany przez administratora mechanizm zgody nie jest zgodny z RODO. Jak wskazano w sekcji 3.1 dotyczącej warunku świadomej zgody, administrator musi poinformować osobę, której dane dotyczą, o prawie do wycofania zgody jeszcze przed faktycznym wyrażeniem zgody zgodnie z art. 7 ust. 3 RODO. Ponadto w ramach obowiązku zapewnienia przejrzystości administrator musi poinformować osoby, których dane dotyczą, o sposobie korzystania z przysługujących im praw[52].

Co do zasady w razie wycofania zgody wszystkie operacje przetwarzania danych, które przeprowadzono w oparciu o tę zgodę przed jej wycofaniem i które były zgodne z RODO, pozostają zgodne z prawem, jednak administrator musi zaprzestać przetwarzania tych danych. Jeżeli nie ma innej zgodnej z prawem podstawy przetwarzania danych (np. dalsze przechowywanie), administrator powinien je usunąć[53].

Jak wskazano wcześniej w niniejszych wytycznych, bardzo ważne jest, aby administratorzy oceniali faktyczne cele przetwarzania danych i zgodne z prawem podstawy takiego przetwarzania przed zgromadzeniem danych. Przedsiębiorstwa często potrzebują danych osobowych do różnych celów, a przetwarzanie opiera się na więcej niż jednej zgodnej z prawem podstawie, np. przetwarzanie danych klientów może odbywać się na podstawie umowy i zgody. Oznacza to, że wycofanie zgody nie jest jednoznaczne z obowiązkiem usunięcia danych przetwarzanych w określonym celu wynikającym z umowy z osobą, której dane dotyczą. W związku z tym administratorzy powinni od początku jasno określić, jaki jest cel przetwarzania konkretnych danych i jaka jest zgodna z prawem podstawa takiego przetwarzania.

Po wycofaniu zgody administratorzy mają obowiązek usunąć dane, które przetwarzano na jej podstawie, zakładając, że nie ma innych celów uzasadniających dalsze ich przechowywanie[54].
Poza tą sytuacją, którą przewidziano w art. 17 ust. 1 lit. b), konkretna osoba, której dane dotyczą, może zażądać usunięcia innych dotyczących jej danych, które są przetwarzanie na innej zgodnej z prawem podstawie, np. na podstawie art. 6 ust. 1 lit. b)[55]. Administratorzy mają obowiązek ocenić, czy dalsze przetwarzanie odnośnych danych jest właściwe, nawet jeżeli osoba, której dane dotyczą, nie zażądała ich usunięcia[56].

Jeżeli osoba, której dane dotyczą, wycofuje swoją zgodę, a administrator chce w dalszym ciągu przetwarzać dane osobowe na innej zgodnej z prawem podstawie, nie może on przejść ze zgody (która zostaje wycofana) na inną zgodną z prawem podstawę bez informowania o tym zainteresowanych osób. Osoba, której dane dotyczą, powinna być informowana o każdej zmianie zgodnej z prawem podstawy przetwarzania zgodnie z wymogami w zakresie informacji określonymi w art. 13 i 14 i zgodnie z ogólną zasadą przejrzystości.

6. Zależność między zgodą a innymi zgodnymi z prawem podstawami, o których mowa w art. 6 RODO

[49] Zob. wytyczne GR29 w sprawie przejrzystości. [Citation to be finalized when available]
[50] GR29 omówiła tę kwestię w swojej opinii na temat zgody (zob. opinia 15/2011 w sprawie definicji zgody (WP 187), s. 9, 13, 20, 27 i 32–33) oraz m.in. w opinii w sprawie wykorzystywania danych dotyczących lokalizacji (zob. opinia 5/2005 w sprawie wykorzystywania danych dotyczących lokalizacji w celu świadczenia usług tworzących wartość dodaną (WP 115), s. 7).
[51] Zob. również opinia 4/2010 Grupy Roboczej Art. 29 na temat europejskiego kodeksu postępowania Europejskiej Federacji Stowarzyszeń Marketingu Bezpośredniego (FEDMA) w sprawie ochrony danych osobowych wykorzystywanych w marketingu bezpośrednim (WP 174) oraz opinia w sprawie wykorzystywania danych dotyczących lokalizacji w celu świadczenia usług tworzących wartość dodaną (WP 115).
[52] Zgodnie z motywem 39 RODO, który odnosi się do art. 13 i 14 tego rozporządzenia, „osobom fizycznym należy uświadomić ryzyka, zasady, zabezpieczenia i prawa związane z przetwarzaniem danych osobowych oraz sposoby wykonywania praw przysługujących im w związku z takim przetwarzaniem".
[53] Zob. art. 17 ust. 1 lit. b) i ust. 3 RODO.
[54] Wówczas pozostałe cele uzasadniające przetwarzanie muszą opierać się na odrębnej podstawie prawnej. Nie oznacza to, że administrator może zastąpić zgodę inną zgodną z prawą podstawą; zob. sekcja 6 poniżej.
[55] Zob. art. 17, w tym wyjątki, które mogą mieć zastosowanie, i motyw 65 RODO.
[56] Zob. również art. 5 ust. 1 lit. e) RODO.

W art. 6 przewidziano warunki zgodnego z prawem przetwarzania danych osobowych i opisano sześć zgodnych z prawem podstaw, na których administrator może się opierać. Zastosowanie jednej z tych sześciu podstaw musi zostać ustalone przed przetwarzaniem i w odniesieniu do określonego celu[57].

W tym miejscu należy wspomnieć, że jeżeli administrator postanowi opierać się na zgodzie w odniesieniu do dowolnej części przetwarzania, musi być gotowy przestrzegać tego wyboru i zaprzestać danej części przetwarzania, jeżeli dana osoba wycofa zgodę. Poinformowanie, że dane będą przetwarzane na podstawie zgody, podczas gdy administrator w praktyce opiera się na innej zgodnej z prawem podstawie, byłoby zdecydowanie nieuczciwe względem zainteresowanych osób.

Innymi słowy, administrator nie może zastąpić zgody innymi zgodnymi z prawem podstawami. Na przykład nie można stosować uzasadnionego interesu z mocą wsteczną jako podstawy uzasadniającej przetwarzanie danych w sytuacji powstania wątpliwości co do ważności zgody. Ze względu na wymóg ujawnienia zgodnej z prawem podstawy, na której opiera się administrator w momencie gromadzenia danych osobowych, administratorzy muszą określić zgodną z prawem podstawę, która będzie miała zastosowanie, jeszcze przed zebraniem danych.

7. Szczególnie istotne obszary w RODO

7.1. Dzieci (art. 8)

W porównaniu z obowiązującą dyrektywą RODO tworzy dodatkową warstwę ochronną w przypadku przetwarzania danych osobowych osób fizycznych wymagających szczególnego traktowania, w szczególności dzieci. W art. 8 wprowadzono dodatkowe obowiązki w celu zapewnienia zwiększonego poziomu ochrony danych dzieci w związku z usługami społeczeństwa informacyjnego. Przyczyny zwiększonej ochrony określono w motywie 38: „[...] mogą one być mniej świadome ryzyka, konsekwencji, zabezpieczeń i praw przysługujących im w związku z przetwarzaniem danych osobowych [...]". W motywie 38 określono również, że „taka szczególna ochrona powinna mieć zastosowanie przede wszystkim do wykorzystywania danych osobowych dzieci do celów marketingowych lub do tworzenia profili osobowych lub profili użytkownika oraz do zbierania danych osobowych dotyczących dzieci, gdy korzystają one z usług skierowanych bezpośrednio do nich". Wyrażenie „przede wszystkim" wskazuje, że szczególna ochrona nie ogranicza się do celów marketingowych lub tworzenia profili, ale obejmuje również szerzej zakrojone „zbieranie danych osobowych dotyczących dzieci".

Art. 8 ust. 1 stanowi, że jeżeli zastosowanie ma zgoda, w przypadku usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku zgodne z prawem jest przetwarzanie danych osobowych dziecka, które ukończyło 16 lat. Jeżeli dziecko nie ukończyło 16 lat, takie przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy zgodę wyraziła lub zatwierdziła osoba sprawująca władzę rodzicielską lub opiekę nad dzieckiem oraz wyłącznie w zakresie wyrażonej zgody[58]. Jeżeli chodzi o granicę wieku, jaka jest niezbędna do wyrażenia ważnej zgody, w RODO przewidziano pewną elastyczność, a państwa członkowskie mogą określić w prawie niższy wiek, jednak nie niższy niż 13 lat.

Jak wskazano w sekcji 3.1 na temat świadomej zgody, informacje powinny być zrozumiałe dla odbiorców, do których zwraca się administrator, przy zwróceniu szczególnej uwagi na sytuację dzieci. Aby uzyskać od dziecka „świadomą zgodę", administrator musi wyjaśnić, jak ma zamiar przetwarzać zgromadzone dane, przy użyciu języka, który jest jasny i zrozumiały dla dzieci[59]. Jeżeli zgodę ma wyrazić rodzic, wówczas może być niezbędny zestaw informacji, który umożliwi osobom dorosłym podjęcie świadomej decyzji.

Z powyższego wyraźnie wynika, że przepisy art. 8 mają zastosowanie wyłącznie wtedy, gdy spełnione są następujące warunki:

- przetwarzanie dotyczy usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku[60][61];
- przetwarzanie jest oparte na zgodzie.

7.1.1. Usługi społeczeństwa informacyjnego

Aby określić zakres pojęcia „usługi społeczeństwa informacyjnego" w RODO, w art. 4 pkt 25 RODO odwołano się do dyrektywy 2015/1535.

Oceniając zakres tej definicji, GR29 odnosi się również do orzecznictwa Trybunału Sprawiedliwości[62]. Trybunał Sprawiedliwości orzekł, że usługi społeczeństwa informacyjnego obejmują umowy i inne usługi, które są zawierane lub świadczone drogą elektroniczną. Jeżeli usługa ma dwa niezależne ekonomicznie komponenty, z których jeden występuje online, takie jak oferta i akceptacja oferty w kontekście zawarcia umowy lub informacji dotyczących produktów lub usług, w tym działań marketingowych, komponent ten jest zdefiniowany jako usługa społeczeństwa

[57] Zgodnie z art. 13 ust. 1 lit. c) lub art. 14 ust. 1 lit. c) administrator musi poinformować o tym osobę, której dane dotyczą.

[58] Niezależnie od możliwości odstępstwa od granicy wieku w prawach państw członkowskich zob. art. 8 ust. 1.

[59] W motywie 58 RODO potwierdzono ten obowiązek, stwierdzając, że administrator powinien zapewnić, by przekazywane informacje były zrozumiałe dla dzieci.

[60] Zgodnie z art. 4 pkt 25 RODO usługa społeczeństwa informacyjnego oznacza usługę w rozumieniu art. 1 ust. 1 lit. b) dyrektywy 2015/1535: „b) »usługa« oznacza każdą usługę społeczeństwa informacyjnego, to znaczy każdą usługę normalnie świadczoną za wynagrodzeniem, na odległość, drogą elektroniczną i na indywidualne żądanie odbiorcy usług. Do celów niniejszej definicji: (i) »na odległość« oznacza, że usługa świadczona jest bez równoczesnej obecności stron; (ii) »drogą elektroniczną« oznacza, iż usługa jest wysyłana i odbierana w miejscu przeznaczenia za pomocą sprzętu elektronicznego do przetwarzania (włącznie z kompresją cyfrową) oraz przechowywania danych, i która jest całkowicie przesyłana, kierowana i otrzymywana za pomocą kabla, fal radiowych, środków optycznych lub innych środków elektromagnetycznych; (iii) »na indywidualne żądanie odbiorcy usług« oznacza, że usługa świadczona jest poprzez przesyłanie danych na indywidualne żądanie". W załączniku I tej dyrektywy podano orientacyjny wykaz usług nieobjętych niniejszą definicją. Zob. także motyw 18 dyrektywy 2000/31.

[61] Zgodnie z art. 1 konwencji ONZ o prawach dziecka „[...] »dziecko« oznacza każdą istotę ludzką w wieku poniżej osiemnastu lat, chyba że zgodnie z prawem odnoszącym się do dziecka uzyska ono wcześniej pełnoletność", zob. rezolucja Zgromadzenia Ogólnego ONZ 44/25 z dnia 20 listopada 1989 r. (konwencja o prawach dziecka).

[62] Zob. wyrok Trybunału Sprawiedliwości z dnia 2 grudnia 2010 r., C-108/09 (Ker-Optika), pkt 22 i 28. W odniesieniu do usług mieszanych GR29 odwołuje się również do pkt 40 wyroku w sprawie C-434/15 (Asociación Profesional Elite Taxi przeciwko Uber Systems Spain SL), w którym stwierdzono, że usługi społeczeństwa informacyjnego stanowiącej integralną część złożonej usługi, której głównym elementem nie jest usługa społeczeństwa informacyjnego (w tym przypadku jest to usługa przewozowa), nie należy kwalifikować jako „usługę społeczeństwa informacyjnego".

informacyjnego, a drugi komponent będący fizyczną dostawą lub dystrybucją towarów nie będzie objęty pojęciem usługi społeczeństwa informacyjnego Świadczenie usługi w trybie online wchodzi w zakres pojęcia usługi społeczeństwa informacyjnego określonej w art. 8 RODO.

7.1.2. Usługi oferowane bezpośrednio dziecku

Sformułowanie „oferowane bezpośrednio dziecku" wskazuje, że art. 8 ma zastosowanie do niektórych, lecz nie do wszystkich usług społeczeństwa informacyjnego. W tym zakresie jeżeli dostawca usług społeczeństwa informacyjnego wyraźnie poinformuje potencjalnych użytkowników, że oferuje swoją usługę wyłącznie osobom, które skończyły 18 lat, i jeżeli inne dowody nie wskazują inaczej (np. treść strony lub plany marketingowe), wówczas usługa nie zostanie uznana za „oferowaną bezpośrednio dziecku", a przepisy art. 8 nie będą miały zastosowania.

7.1.3. Wiek

RODO stanowi, że „państwa członkowskie mogą przewidzieć w swoim prawie niższą granicę wiekową, która musi wynosić co najmniej 13 lat". Administrator musi być świadomy różnic w przepisach krajowych, uwzględniając docelową grupę odbiorców jego usług. W szczególności należy zauważyć, że administrator świadczący usługę transgraniczną nie zawsze może polegać wyłącznie na zgodności z prawem państwa członkowskiego, w którym ma swoją główną jednostkę organizacyjną, ale może być zobowiązany do przestrzegania odpowiednich przepisów krajowych każdego państwa członkowskiego, w którym oferuje usługę lub usługi społeczeństwa informacyjnego. Zależy to od tego, czy państwo członkowskie wybierze – jako punkt odniesienia w prawie krajowym – miejsce głównej jednostki organizacyjnej administratora czy też miejsce zamieszkania osoby, której dane dotyczą. Państwa członkowskie, przy podejmowaniu tej decyzji, powinny brać pod uwagę przede wszystkim dobro dziecka. Grupa Robocza zachęca państwa członkowskie do poszukiwania zharmonizowanego rozwiązania w tym zakresie.

Świadcząc dzieciom usługi społeczeństwa informacyjnego na podstawie zgody, administratorzy powinni podjąć rozsądne starania, by zweryfikować, czy użytkownik osiągnął wiek uprawniający do wyrażenia zgody drogą elektroniczną, przy czym starania te powinny być proporcjonalne do charakteru czynności przetwarzania i związanego z nimi ryzyka.

Jeżeli użytkownicy oświadczą, że są w wieku uprawniającym do wyrażenia zgody drogą elektroniczną, wówczas administrator może podjąć właściwe czynności kontrolne, by zweryfikować, czy te oświadczenia są prawdziwe. Chociaż w RODO nie wskazano wyraźnie konieczności podjęcia rozsądnych starań w celu zweryfikowania wieku, jest to w sposób dorozumiany wymagane, ponieważ jeżeli dziecko wyrazi zgodę, a nie osiągnęło wystarczającego wieku, aby udzielić ważnej zgody we własnym imieniu, taka czynność sprawi, to spowoduje to niezgodność z prawem przetwarzania danych.

Jeżeli użytkownik oświadczy, że nie osiągnął wieku uprawniającego do wyrażenia zgody drogą cyfrową, administrator może przyjąć takie oświadczenie bez konieczności podejmowania dalszych działań kontrolnych, ale będzie musiał przejść do uzyskania zgody rodzica lub opiekuna i zweryfikować, że osoba udzielająca takiej zgody sprawuje władzę rodzicielską lub opiekę nad dzieckiem.

Weryfikacja wieku nie powinna prowadzić do nadmiernego przetwarzania danych. Mechanizm wybrany do weryfikacji wieku osoby, której dane dotyczą, powinien obejmować ocenę ryzyka związanego z proponowanym przetwarzaniem. W niektórych sytuacjach niskiego ryzyka właściwe może być zobowiązanie nowego abonenta usługi do ujawnienia roku urodzenia lub wypełnienia formularza, w którym oświadczy, że (nie) jest osobą małoletnią[63]. W razie wątpliwości administrator powinien przeanalizować swoje mechanizmy weryfikacji wieku w danym przypadku i rozważyć, czy niezbędne są alternatywne sposoby weryfikacji[64].

7.1.4. Zgoda udzielana przez dzieci i władza rodzicielska

Jeżeli chodzi o potwierdzenie przez osobę sprawującą władzę rodzicielską lub opiekę nad dzieckiem, w RODO nie wskazano konkretnych praktycznych sposobów na uzyskanie zgody rodzica lub ustalenie, że dana osoba jest uprawniona do podjęcia takiej czynności[65]. W związku z tym GR29 zaleca przyjęcie proporcjonalnego podejścia zgodnie z art. 8 ust. 2 i art. 5 ust. 1 lit. c) RODO (minimalizacja danych). Stosując proporcjonalne podejście, można skupić się na uzyskaniu ograniczonej ilości informacji, np. danych kontaktowych rodzica lub opiekuna.

Racjonalność działań podejmowanych w celu weryfikacji, czy dany użytkownik osiągnął odpowiedni wiek do samodzielnego wyrażenia zgody oraz czy osoba wyrażająca zgodę w imieniu dziecka sprawuje władzę rodzicielską lub opiekę nad dzieckiem, może zależeć od ryzyka związanego z przetwarzaniem oraz od dostępnej technologii. W sytuacjach niskiego ryzyka może wystarczyć weryfikacja posiadania władzy rodzicielskiej za pośrednictwem poczty elektronicznej. W sytuacjach wysokiego ryzyka właściwe może być natomiast poproszenie o więcej dowodów, tak by administrator był w stanie zweryfikować i przechowywać informacje zgodnie z art. 7 ust. 1 RODO[66]. Zaufani zewnętrzni dostawcy usług weryfikacyjnych mogą oferować rozwiązania, które zminimalizują ilość danych osobowych wymaganych przez administratora w celu weryfikacji wieku.

> [Przykład 23] Platforma gier online chce mieć pewność, że małoletni klienci subskrybują jej usługi wyłącznie za zgodą swoich rodziców lub opiekunów. Administrator podejmuje następujące kroki:
> krok 1: prosi użytkownika o oświadczenie, czy osiągnął wiek 16 lat (lub inny wiek uprawniający do wyrażenia zgody drogą elektroniczną).
> Jeżeli użytkownik oświadczy, że nie osiągnął wieku uprawniającego do wyrażenia zgody drogą elektroniczną:
> krok 2: platforma informuje dziecko, że rodzic lub opiekun musi wcześniej wyrazić zgodę lub zezwolić na przetwarzanie danych dziecka, zanim nastąpi świadczenie usługi dziecku. Użytkownik jest proszony o podanie adresu e-mail rodzica lub opiekuna;

[63] Chociaż nie zawsze to rozwiązanie jest pozbawione wad, jest to przykład tego, jak można dopełnić wymogu wynikającego z tego przepisu.
[64] Zob. opinia GR29 5/2009 w sprawie portali społecznościowych (WP 163).
[65] GR29 zauważa, że nie zawsze osoba sprawująca władzę rodzicielską lub opiekę nad dzieckiem jest rodzicem biologicznym dziecka i że władzę rodzicielską może sprawować wiele osób, w tym osoby prawne i fizyczne.
[66] Przykładowo rodzic lub opiekun może zostać poproszony o dokonanie płatności w wysokości 0,01 EUR na rzecz administratora za pomocą przelewu bankowego, w tym o krótkie potwierdzenie w opisie transakcji, że posiadacz rachunku bankowego sprawuje władzę rodzicielską lub opiekę nad użytkownikiem. W stosownych przypadkach należy zapewnić alternatywną metodę weryfikacji, aby zapobiec nieuzasadnionemu dyskryminacyjnemu traktowaniu osób, które nie posiadają rachunku bankowego.

krok 3: platforma kontaktuje się z rodzicem lub opiekunem i za pośrednictwem poczty elektronicznej uzyskuje od niego zgodę na przetwarzanie, a także podejmuje niezbędne działania w celu potwierdzenia, że osoba dorosła sprawuje władzę rodzicielską lub opiekę nad użytkownikiem;
Krok 4: w przypadku skarg platforma podejmuje dodatkowe działania w celu weryfikacji wieku abonenta.
Jeżeli platforma spełniła pozostałe wymogi dotyczące zgody, może ona spełnić dodatkowe kryteria przewidziane w art. 8 RODO, podejmując powyższe kroki.

Przykład pokazuje, że administrator może zadbać o to, aby móc wykazać, że podjął rozsądne starania w celu uzyskania ważnej zgody w odniesieniu do usług oferowanych dzieciom. W art. 8 ust. 2 w szczególności dodano, że „administrator, uwzględniając dostępną technologię, podejmuje rozsądne starania, by zweryfikować, czy osoba sprawująca władzę rodzicielską lub opiekę nad dzieckiem wyraziła zgodę lub ją zaaprobowała".

Do administratora należy ustalenie, jakie środki są odpowiednie w konkretnym przypadku. Co do zasady administratorzy powinni unikać rozwiązań w zakresie weryfikacji, które same w sobie wymagają nadmiernego zbierania danych osobowych.

GR29 przyznaje, że mogą istnieć sytuacje, w których weryfikacja stanowić będzie wyzwanie (np. jeżeli dzieci, które wyraziły zgodę, nie utworzyły wcześniej „śladu tożsamości" lub gdy potwierdzenie władzy rodzicielskiej jest utrudnione). Można to uwzględnić przy podejmowaniu decyzji o tym, które starania są rozsądne, ale oczekuje się również, że administratorzy będą poddawać swoje procesy i dostępną technologię ciągłym przeglądom.

Jeżeli chodzi o samodzielność osoby, której dane dotyczą, w wyrażeniu zgody na przetwarzanie jej danych osobowych i jej pełną kontrolę nad przetwarzaniem, zgoda udzielona przez osobę sprawującą władzę rodzicielską lub opiekę nad dzieckiem bądź pozwolenie na przetwarzanie danych osobowych dzieci udzielone przez taką osobę mogą zostać potwierdzone, zmienione lub wycofane po osiągnięciu przez osobę, której dane dotyczą, wieku uprawniającego do wyrażenia zgody drogą elektroniczną.
W praktyce oznacza to, że jeżeli dziecko nie podejmuje żadnych działań, zgoda udzielona przez osobę sprawującą władzę rodzicielską lub opiekę nad dzieckiem lub pozwolenie na przetwarzanie danych osobowych udzielone przez osobę sprawującą władzę lub opiekę rodzicielską nad dzieckiem przed osiągnięciem przez dziecko wieku uprawniającego do wyrażenia zgody drogą elektroniczną pozostaje ważną podstawą przetwarzania danych.
Po osiągnięciu wieku uprawniającego do wyrażenia zgody drogą elektroniczną dziecko będzie mogło samodzielnie wycofać zgodę zgodnie z art. 7 ust. 3. Zgodnie z zasadami uczciwości i odpowiedzialności administrator musi poinformować dziecko o takiej możliwości[67].

Należy podkreślić, że zgodnie z motywem 38 zgoda rodzica lub opiekuna nie jest wymagana w przypadku usług profilaktycznych lub doradczych oferowanych bezpośrednio dziecku. Na

[67] Ponadto osoba, której dane dotyczą, powinna zdawać sobie sprawę z posiadania prawa do bycia zapomnianym zgodnie z art. 17, co jest szczególnie istotne w przypadku zgody udzielonej, kiedy osoba, której dane dotyczą, była jeszcze dzieckiem; zob. motyw 63.

przykład świadczenie dziecku usług z zakresu ochrony dziecka za pośrednictwem czatu internetowego nie wymaga wcześniejszej zgody rodzica.

Ponadto w RODO określono, że przepisy dotyczące wymogów udzielania zgody przez rodziców lub opiekunów w odniesieniu do małoletnich nie powinny wpływać na „ogólne przepisy prawa umów państw członkowskich, takie jak przepisy o ważności, zawieraniu lub skutkach umowy wobec dziecka". W związku z tym wymogi w zakresie ważnej zgody na wykorzystywanie danych dotyczących dzieci są częścią ram prawnych, które należy postrzegać jako odrębne od krajowego prawa umów. W niniejszych wytycznych nie poruszono zatem kwestii tego, czy małoletni mogą zgodnie z prawem zawierać umowy przez internet. Oba systemy prawne mogą mieć jednocześnie zastosowanie, a zakres zastosowania RODO nie obejmuje ujednolicenia przepisów krajowych prawa umów.

7.2. Badania naukowe

Definicja celów badań naukowych ma istotne konsekwencje dla szeregu czynności przetwarzania danych, które może podejmować administrator. Termin „badania naukowe" nie jest zdefiniowany w RODO. Motyw 159 stanowi, że „(...) W niniejszym rozporządzeniu przetwarzanie danych osobowych do celów badań naukowych należy interpretować szeroko (...)", GR29 uważa jednak, że pojęcia tego nie można rozciągać poza jego powszechne znaczenie, i jest zdania, że w tym kontekście „badania naukowe" oznaczają projekt badawczy zorganizowany zgodnie z odpowiednimi normami metodycznymi i etycznymi w danym sektorze oraz zgodnie z dobrymi praktykami.

Jeżeli podstawą prawną do przeprowadzenia badań zgodnie z RODO jest zgoda, należy odróżnić taką zgodę na wykorzystywanie danych osobowych od innych wymogów w zakresie zgody, które stanowią normę etyczną lub obowiązek proceduralny. Przykłady takich obowiązków proceduralnych, w których przetwarzanie odbywa się na innej podstawie prawnej niż zgoda, znajdują się w rozporządzeniu w sprawie badań klinicznych. W kontekście prawa w dziedzinie ochrony danych taką formę zgody można traktować jako dodatkowe zabezpieczenie[68]. Jednocześnie w odniesieniu do przetwarzania danych do celów badań RODO nie ogranicza zastosowania art. 6 wyłącznie do zgody. Możliwe są inne podstawy prawne, takie jak art. 6 ust. 1 lit. e) lub f)[69], jeżeli istnieją właściwe zabezpieczenia, np. wymogi przewidziane w art. 89 ust. 1, a przetwarzanie jest uczciwe, zgodne z prawem, przejrzyste oraz zgodne z normami w zakresie minimalizacji danych i prawami poszczególnych osób. Dotyczy to również szczególnych kategorii danych zgodnie z odstępstwem, o którym mowa w art. 9 ust. 2 lit. j)[70].

Wydaje się, że w motywie 33 wprowadzono pewną elastyczność co do stopnia specjalizacji i szczegółowości zgody w kontekście badań naukowych. Motyw 33 stanowi, że: „w momencie

[68] Zob. również motyw 161 RODO.
[69] Przepisy art. 6 ust. 1 lit. c) mogą mieć zastosowanie również do części operacji przetwarzania, które są szczególnie wymagane przez prawo, np. do zbierania wiarygodnych i solidnych danych zgodnie z protokołem zatwierdzonym przez dane państwo członkowskie na podstawie rozporządzenia w sprawie badań klinicznych.
[70] Określone testy produktów leczniczych mogą odbywać się zgodnie z przepisami unijnymi lub prawem krajowym na podstawie art. 9 ust. 2 lit. i).

zbierania danych często nie da się w pełni zidentyfikować celu przetwarzania danych osobowych na potrzeby badań naukowych. Dlatego osoby, których dane dotyczą, powinny móc wyrazić zgodę na niektóre obszary badań naukowych, o ile badania te są zgodne z uznanymi normami etycznymi w zakresie badań naukowych. Osoby, których dane dotyczą, powinny móc wyrazić zgodę tylko na niektóre obszary badań lub elementy projektów badawczych, o ile umożliwia to zamierzony cel".

Po pierwsze należy zauważyć, że motyw 33 nie uchyla obowiązków dotyczących wymogu uzyskania konkretnej zgody. Oznacza to, że w projektach badań naukowych można zasadniczo wykorzystywać dane osobowe na podstawie zgody tylko wtedy, gdy właściwie opisano ich cel. W przypadku projektów badań naukowych, w odniesieniu do których nie można z góry określić szczegółowo celów przetwarzania danych, w motywie 33 przewidziano wyjątek, zgodnie z którym cel można opisać bardziej ogólnie.

Mając na uwadze rygorystyczne warunki, które ustanowiono w art. 9 RODO w odniesieniu do przetwarzania szczególnych kategorii danych, GR29 zauważa, że w przypadku przetwarzania szczególnych kategorii danych w oparciu o wyraźną zgodę zastosowanie elastycznego podejścia zgodnie z motywem 33 powinno być interpretowane bardziej zawężająco i wymaga wysokiego stopnia kontroli.

W ujęciu ogólnym RODO nie może być interpretowane w sposób umożliwiający administratorowi obejście zasadniczej zasady szczegółowego określenia celów, w odniesieniu do których prosi się o zgodę osoby, której dane dotyczą.
Jeżeli nie można w pełni określić celów badań, administrator musi szukać innych sposobów zapewnienia, aby jak najlepiej zrealizować istotę wymogów w zakresie zgody, np. umożliwić osobom, których dane dotyczą, udzielenie zgody na dany cel badania określony bardziej ogólnie oraz umożliwić realizację poszczególnych etapów projektu badawczego, które znane są już na początku. W miarę postępu badań przed rozpoczęciem kolejnego etapu można uzyskać zgodę na następne etapy projektu. Taka zgoda nadal powinna być jednak zgodna z mającymi zastosowanie normami etycznymi w zakresie badań naukowych.

Ponadto administrator może ustanowić w takich przypadkach dodatkowe zabezpieczenia. Przykładowo w art. 89 ust. 1 podkreślono konieczność ustanowienia zabezpieczeń w zakresie czynności przetwarzania danych do celów badań naukowych lub historycznych lub do celów statystycznych. Cele te powinny podlegać „odpowiednim zabezpieczeniom dla praw i wolności osoby, której dane dotyczą, zgodnie z niniejszym rozporządzeniem". Wśród możliwych zabezpieczeń wymieniono minimalizację danych, anonimizację i zapewnienie bezpieczeństwa danych[71]. Anonimizacja jest preferowanym rozwiązaniem na etapach, gdy cel badania można osiągnąć bez przetwarzania danych osobowych.

[71] Zob. np. motyw 156. Przetwarzanie danych osobowych do celów naukowych powinno też być zgodne z innymi odpowiednimi przepisami, takimi jak przepisy o próbach klinicznych; zob. motyw 156, w którym jest mowa o rozporządzeniu Parlamentu Europejskiego i Rady (UE) nr 536/2014 z dnia 16 kwietnia 2014 r. w sprawie badań klinicznych produktów leczniczych stosowanych u ludzi. Zob. również opinia GR29 15/2011 w sprawie definicji zgody (WP 187), s. 7: „Ponadto uzyskanie zgody nie zwalnia administratora danych z obowiązków na mocy art. 6 związanych z rzetelnością, koniecznością i proporcjonalnością, jak też jakością danych. Na przykład nawet jeżeli użytkownik

Przejrzystość jest dodatkowym zabezpieczeniem, jeżeli okoliczności badania nie pozwalają na uzyskanie konkretnej zgody. Aby zrekompensować brak uszczegółowienia celu, administratorzy mogą regularnie podawać informacje na temat rozwoju celu w miarę postępu projektu badawczego, tak aby z czasem zgoda była tak konkretna, jak to tylko możliwe. W ten sposób osoba, której dane dotyczą, ma przynajmniej podstawowy obraz aktualnej sytuacji, dzięki czemu może ocenić, czy np. powinna skorzystać z prawa cofnięcia zgody na podstawie art. 7 ust. 3[72].

Brak uszczegółowienia celu można zrekompensować również poprzez udostępnienie do wglądu kompleksowego planu badawczego osobom, których dane dotyczą, zanim wyrażą one zgodę[73]. W takim planie badawczym należy jak najbardziej szczegółowo określić badane zagadnienia i przewidywane metody pracy. Plan badawczy może również pomóc w zapewnieniu zgodności z przepisami art. 7 ust. 1, ponieważ aby móc udowodnić, że uzyskana zgoda jest ważna, administratorzy muszą wskazać, jakie informacje były dostępne dla osób, których dane dotyczą, w momencie udzielania przez nich zgody.

Należy przypomnieć, że jeżeli zgoda jest stosowana jako zgodna z prawem podstawa przetwarzania, osoba, której dane dotyczą, musi mieć możliwość wycofania tej zgody. GR29 zauważa, że wycofanie zgody może podważyć te rodzaje badań naukowych, które wymagają danych, które można powiązać z poszczególnymi osobami; w RODO jednak wyraźnie przewidziano możliwość wycofania takiej zgody, a administratorzy muszą odpowiednio reagować na takie działanie – w rozporządzeniu nie przewidziano odstępstwa od tego wymogu w przypadku badań naukowych. Jeśli administrator otrzyma żądanie wycofania zgody, musi zasadniczo bezzwłocznie usunąć dane osobowe, jeżeli chce w dalszym ciągu wykorzystywać dane do celów badania[74].

7.3. Prawa osób, których dane dotyczą

Jeżeli czynność przetwarzania danych opiera się na zgodzie osoby, której dane dotyczą, będzie to miało wpływ na prawa tej osoby. Osoby, której dane dotyczą, mogą mieć prawo do przenoszenia danych (art. 20), gdy przetwarzanie odbywa się w oparciu o zgodę. Natomiast prawo do sprzeciwu (art. 21) nie ma zastosowania, jeżeli przetwarzanie odbywa się w oparciu o zgodę, jednak prawo do wycofania zgody w dowolnym momencie może wywołać podobne skutki.

wyraził zgodę na przetwarzanie danych osobowych, nie czyni to legalnym gromadzenia danych nadmiernych w stosunku do określonego celu. [...] Co do zasady, zgody nie należy uważać za odstępstwo od pozostałych zasad ochrony danych, lecz za zabezpieczenie. Jest ona przede wszystkim podstawą do zapewnienia zgodności z prawem i nie zwalnia z obowiązku stosowania innych zasad".
[72] Istotne mogą być również inne środki na rzecz przejrzystości. Jeżeli administratorzy przetwarzają dane do celów naukowych, a przekazanie wszystkich informacji na początku nie jest możliwe, mogą wyznaczyć konkretną osobę do kontaktu dla osób, których dane dotyczą, aby mogły one kierować do niej swoje pytania.
[73] Możliwość taką przewidziano w art. 14 ust. 1 obowiązującej fińskiej ustawy o danych osobowych (Henkilötietolaki, 523/1999).
[74] Opinia GR29 05/2014 w sprawie technik anonimizacji (WP 216).

Zgodnie z art. 16–20 RODO (jeżeli przetwarzanie danych odbywa się w oparciu o zgodę) osoby, których dane dotyczą, mają prawo do usunięcia danych, jeżeli zgoda została wycofana, oraz prawo do ograniczenia przetwarzania, sprostowania danych i dostępu do danych[75].

8. Zgoda uzyskana na mocy dyrektywy 95/46/WE

Od administratorów, którzy obecnie przetwarzają dane w oparciu o zgodę zgodnie z krajowym prawem w dziedzinie ochrony danych, nie wymaga się automatycznie całkowitego odświeżenia wszystkich istniejących stosunków w zakresie zgody z osobami, których dane dotyczą, w ramach przygotowań do wdrożenia RODO. Zgoda, którą uzyskano do tego czasu, pozostaje ważna w zakresie, w jakim jest ona zgodna z warunkami określonymi w RODO.

Ważne jest, aby przed dniem 25 maja 2018 r. administratorzy dokonali szczegółowego przeglądu obecnych procesów operacyjnych i rejestrów, aby zapewnić zgodność istniejących treści z normami określonymi w RODO (zob. motyw 171 RODO[76]). W praktyce RODO podnosi poprzeczkę w odniesieniu do wdrażania mechanizmów zgody i wprowadzono szereg nowych wymogów, których spełnienie narzuca administratorom konieczność zmiany mechanizmów zgody, a nie tylko przeredagowania polityk prywatności[77].

Na przykład ponieważ zgodnie z RODO administrator musi być wstanie wykazać, że uzyskał ważną zgodę, wszelkie domniemane zgody, w przypadku których nie przechowuje się żadnych odniesień, automatycznie nie będą spełniać standardu zgody na mocy RODO i będą musiały zostać odnowione. Podobnie ponieważ RODO wymaga „oświadczenia lub wyraźnego działania potwierdzającego", wszelkie domniemane zgody, które oparto na bardziej dorozumianej formie działania ze strony osoby, której dane dotyczą (np. domyślnie zaznaczone okienko zgody), również nie będą spełniać standardu normy na mocy RODO.

Ponadto konieczny może być przegląd czynności i systemów informatycznych, aby móc wykazać uzyskanie zgody lub umożliwić bardziej szczegółowe okazanie woli przez osoby, których dane dotyczą. Ponadto należy zapewnić łatwy dostęp do mechanizmów wycofania zgody przez osoby, których dane dotyczą, oraz informacje na temat tego, jak wycofać zgodę. Jeżeli istniejące procedury uzyskiwania zgody i zarządzania zgodą nie spełniają standardów RODO, administratorzy będą musieli uzyskać nową zgodę zgodną z RODO.

[75] W przypadkach, w których zgodnie z art. 18 RODO niektóre czynności przetwarzania danych zostają ograniczone, usunięcie takich ograniczeń może wymagać zgody osoby, której dane dotyczą.
[76] Motyw 171 RODO stanowi, że: „Niniejszym rozporządzeniem należy uchylić dyrektywę 95/46/WE. Przetwarzanie, które w dniu rozpoczęcia stosowania niniejszego rozporządzenia już się toczy, powinno w terminie dwóch lat od wejścia niniejszego rozporządzenia w życie zostać dostosowane do jego przepisów. Jeżeli przetwarzanie ma za podstawę zgodę w myśl dyrektywy 95/46/WE, osoba, której dane dotyczą, nie musi ponownie wyrażać zgody, jeżeli pierwotny sposób jej wyrażenia odpowiada warunkom niniejszego rozporządzenia; dzięki temu administrator może kontynuować przetwarzanie po dacie rozpoczęcia stosowania niniejszego rozporządzenia. Decyzje przyjęte przez Komisję oraz zezwolenia wydane przez organy nadzorcze na podstawie dyrektywy 95/46/WE pozostają w mocy do czasu ich zmiany, zastąpienia lub uchylenia".
[77] Jak wskazano we wprowadzeniu, w RODO jeszcze bardziej sprecyzowano i uszczegółowiono wymogi dotyczące uzyskania ważnej zgody oraz wykazania jej wyrażenia. Wiele nowych wymogów opiera się na opinii 15/2011 w sprawie definicji zgody.

Z drugiej strony ponieważ nie wszystkie elementy przewidziane w art. 13 i 14 muszą być zawsze występować jako warunek świadomej zgody, rozszerzone obowiązki w zakresie informacji, o których mowa w RODO, niekoniecznie naruszają ciągłość zgody wyrażonej przed wejściem RODO w życie (zob. s. 15 powyżej). W dyrektywie 95/46/WE nie przewidziano obowiązku informowania osób, których dane dotyczą, o podstawach, na których prowadzono przetwarzanie.

Jeżeli administrator ustali, że zgoda uzyskana wcześniej na podstawie dawnych przepisów nie będzie spełniać standardu zgody na mocy RODO, wówczas musi on podjąć działania w celu zapewnienia zgodności z tymi standardami, np. przez odnowienie zgody w sposób zgodny z RODO. W RODO nie przewidziano możliwości zastąpienia jednej zgodnej z prawem podstawą inną podstawą. Jeżeli administrator nie jest w stanie odnowić zgody w sposób zgodny z RODO i nie jest także w stanie osiągnąć zgodności z RODO przez oparcie przetwarzania danych na innej zgodnej z prawem podstawie przy jednoczesnym zapewnieniu, by dalsze przetwarzanie odbywało się w sposób uczciwy i odpowiedzialny (przy czym taka niemożliwość osiągnięcia zgodności jest przypadkiem jednorazowym), musi zaprzestać czynności przetwarzania. W każdym przypadku administrator musi przestrzegać zasad zgodnego z prawem, uczciwego i przejrzystego przetwarzania danych.

-*-*-*-*-*-*-*-*-*-*-* **KONIEC DOKUMENTU** *-*

GRUPA ROBOCZA ART. 29

17/PL

GR260 rev.01

Grupa Robocza Art. 29

Wytyczne w sprawie przejrzystości na podstawie rozporządzenia 2016/679

Przyjęte dnia 29 listopada 2017 r.

Ostatnio zmienione i przyjęte w dniu 11 kwietnia 2018 r.

GRUPA ROBOCZA DS. OCHRONY OSÓB FIZYCZNYCH W ZAKRESIE

PRZETWARZANIA DANYCH OSOBOWYCH

powołana na podstawie dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r.,

uwzględniając art. 29 i 30 tej dyrektywy,

uwzględniając swój regulamin wewnętrzny,

PRZYJMUJE NINIEJSZE WYTYCZNE:

Grupa Robocza została powołana na podstawie art. 29 dyrektywy 95/46/WE. Jest ona niezależnym europejskim organem doradczym w zakresie ochrony danych i prywatności. Zadania Grupy zostały określone w przepisach art. 30 dyrektywy 95/46/WE i art. 15 dyrektywy 2002/58/WE.

Obsługę sekretariatu zapewnia Komisja Europejska, Dyrekcja C (Prawa Podstawowe i Obywatelstwo Unii Europejskiej) Dyrekcji Generalnej ds. Sprawiedliwości, B-1049 Bruksela, Belgia, biuro nr MO-59 02/013.

Strona internetowa: http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358&tpa_id=6936

GRUPA ROBOCZA ART. 29

Spis treści

Wprowadzenie **4**
Znaczenie przejrzystości **6**
Elementy przejrzystości w świetle RODO **7**
Zwięzła, przejrzysta, zrozumiała i łatwo dostępna forma 7
Jasny i prosty język 9
Udzielanie informacji dzieciom i innym osobom wymagającym szczególnego traktowania 11
Na piśmie lub w inny sposób 12
...informacji można udzielić ustnie... 14
Wolne od opłat 15
Informacje udzielane osobie, której dane dotyczą – art. 13 i 14 ..... **15**
Treść 15
Odpowiednie środki 16
Czas podawania informacji 16
Zmiany w informacjach, o których mowa w art. 13 i 14 19
Terminy powiadamiania o zmianach w informacjach, o których mowa w art. 13 i 14 19
Tryb i format udzielania informacji 21
Warstwowe podejście w otoczeniu cyfrowym i warstwowe oświadczenia o ochronie prywatności / warstwowe informacje o polityce prywatności 21
Warstwowe podejście w otoczeniu innym niż cyfrowe 23
Powiadomienia typu „push" i „pull" 23
Inne rodzaje „odpowiednich środków" 24
Informacje dotyczące profilowania i zautomatyzowanego podejmowania decyzji 25
Inne kwestie – ryzyko, zasady i zabezpieczenia 26
Informacje związane z dalszym przetwarzaniem **27**
Narzędzia wizualizacyjne **28**
Znaki graficzne 29
Mechanizmy certyfikacji, znaki jakości i oznaczenia 30
Wykonywanie uprawnień przysługujących osobom, których dane dotyczą **30**
Wyjątki od obowiązku udzielenia informacji **31**
Wyjątki określone w art. 13 31

Wyjątki określone w art. 14 32
Okazuje się niemożliwe, niewspółmiernie duży wysiłek oraz poważne utrudnienie realizacji celów ..33
„Okazuje się niemożliwe" 33
Niemożność podania źródła danych 34
„Niewspółmiernie duży wysiłek" 34
Poważne utrudnienie realizacji celów 36
Pozyskiwanie lub ujawnianie jest wyraźnie uregulowane w prawie 37
Poufność wynikająca z obowiązku zachowania tajemnicy 38
Ograniczenia praw osoby, której dane dotyczą **39**
Przejrzystość oraz naruszenie ochrony danych **40**
Załącznik **41**

GRUPA ROBOCZA ART. 29

Wprowadzenie

1. Niniejsze wytyczne Grupy Roboczej Art. 29 (GR29) zapewniają praktyczne wskazówki i pomoc w interpretacji w zakresie nowego obowiązku zachowania przejrzystości w odniesieniu do przetwarzania danych osobowych na podstawie ogólnego rozporządzenia o ochronie danych[1] („**RODO**"). Przejrzystość stanowi nadrzędny obowiązek wynikający z RODO, który ma zastosowanie do trzech głównych obszarów: 1) informowania osób, których dane dotyczą, w odniesieniu do rzetelności przetwarzania; 2) sposobu, w jaki administratorzy danych kontaktują się z osobami, których dane dotyczą, w związku z ich prawami wynikającymi z RODO; oraz 3) sposobu, w jaki administratorzy danych ułatwiają wykonywanie praw osobom, których dane dotyczą[2]. W zakresie, w jakim spełnienie wymogu przejrzystości jest konieczne w odniesieniu do przetwarzania danych na podstawie dyrektywy (UE) 2016/680[3], niniejsze wytyczne mają zastosowanie również do wykładni tej zasady[4]. Podobnie jak w przypadku wszystkich wytycznych GR29 również te wytyczne mają mieć ogólne zastosowanie i znaczenie dla administratorów bez względu na specyfikę sektorów, branż lub przepisów, z którymi mają do czynienia administratorzy danych. Ze względu na charakter wytycznych nie można w nich było uwzględnić niuansów i wielu zmiennych, które mogą wystąpić w kontekście obowiązków zapewnienia przejrzystości w danym sektorze, branży lub obszarze podlegającym regulacjom. Celem tych wytycznych jest jednak umożliwienie administratorom zrozumienia – na ogólnym poziomie – sposobu, w jaki GR29 interpretuje praktyczne skutki obowiązków zapewnienia przejrzystości, i wskazanie podejścia, które – zdaniem GR29 – administratorzy powinni przyjąć, aby wprowadzić przejrzystość, a ich działania opierały się na rzetelności i rozliczalności.

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.

[2] W niniejszych wytycznych określono ogólne zasady dotyczące wykonywania praw przez osoby, których dane dotyczą. Nie omówiono w nich natomiast szczególnych warunków związanych z poszczególnymi prawami osób fizycznych, których dane dotyczą, wynikającymi z RODO.

[3] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW.

[4] Chociaż przejrzystość nie jest jedną z zasad dotyczących przetwarzania danych osobowych, które określono w art. 4 dyrektywy (UE) 2016/680, w motywie 26 stwierdzono, że przetwarzanie danych osobowych musi być „zgodne z prawem, rzetelne i przejrzyste" względem zainteresowanej osoby fizycznej.

2. Przejrzystość od wielu lat jest stałym elementem prawa Unii[5]. Jej celem jest zapewnienie zaufania do procesów, które mają wpływ na obywatela, dzięki umożliwieniu mu ich zrozumienia, a w razie konieczności również zgłoszenia wobec nich sprzeciwu. Stanowi również wcielenie zasady rzetelności w odniesieniu do przetwarzania danych osobowych, o którym mowa w art. 8 Karty praw podstawowych Unii Europejskiej. Na podstawie RODO (art. 5 ust. 1 lit. a)[6]) fundamentalnym aspektem tych zasad stała się – obok wymogu zgodnego z prawem i rzetelnego przetwarzania danych – także przejrzystość[7]. Przejrzystość jest nierozerwalnie związana z rzetelnością i nową zasadą rozliczalności w świetle RODO. Ponadto z art. 5 ust. 2 wynika, że administrator musi zawsze być w stanie wykazać, że dane osobowe są przetwarzane w sposób przejrzysty dla osoby, której dane dotyczą[8]. Powiązana z tym zasada rozliczalności wymaga przejrzystości operacji przetwarzania, aby administratorzy danych byli w stanie wykazać, że przestrzegają swoich obowiązków wynikających z RODO[9].

3. Zgodnie z motywem 171 RODO, jeżeli przetwarzanie ma już miejsce w dniu 25 maja 2018 r., administrator danych powinien zapewnić, by od dnia 25 maja 2018 r. odbywało się ono zgodnie z obowiązkami zapewnienia przejrzystości (i ze wszystkimi innymi obowiązkami wynikającymi z RODO). Oznacza to, że przed dniem 25 maja 2018 r. administratorzy danych powinni zrewidować wszystkie informacje podawane osobom, których dane dotyczą, na temat przetwarzania ich danych osobowych (np. w oświadczeniach o ochronie prywatności / informacjach o polityce prywatności itd.), aby zapewnić ich zgodność z wymogami w zakresie przejrzystości omówionymi w niniejszych wytycznych. Jeżeli takie informacje są zmieniane lub uzupełniane, administratorzy powinni wyraźnie poinformować osoby, których dane dotyczą, że zmian tych dokonano w celu zapewnienia zgodności z przepisami RODO. GR29 zaleca czynne powiadamianie o takich zmianach lub uzupełnieniach osób, których dane dotyczą, a przynajmniej publiczne udostępnianie takich informacji przez administratorów (np. na swoich stronach internetowych). Jeżeli jednak zmiany lub uzupełnienia są istotne lub znaczne, wówczas zgodnie z pkt 29–32 poniżej osoba, której dane dotyczą, musi zostać o nich czynnie powiadomiona.

[5] W art. 1 TUE odniesiono się do podejmowania decyzji „z możliwie najwyższym poszanowaniem zasady otwartości i jak najbliżej obywateli"; w art. 11 ust. 2 stwierdzono, że „instytucje utrzymują otwarty, przejrzysty i regularny dialog ze stowarzyszeniami przedstawicielskimi i społeczeństwem obywatelskim"; w art. 15 TFUE mowa jest m.in. o prawie obywateli Unii do dostępu do dokumentów instytucji, organów i jednostek organizacyjnych Unii oraz o wymogach, zgodnie z którymi te instytucje, organy i jednostki organizacyjne Unii mają obowiązek zapewnić przejrzystość swoich prac.

[6] Dane osobowe muszą być „przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą".

[7] W dyrektywie 95/46/WE do przejrzystości nawiązano tylko w motywie 38, wspominając o warunku zapewnienia rzetelności przetwarzania danych, ale w odpowiadających temu motywowi przepisach art. 6 ust. 1 lit. a) nie ma wyraźnego odniesienia do przejrzystości.

[8] Zgodnie z art. 5 ust. 2 RODO administrator danych ma obowiązek wykazać przejrzystość (wraz z pięcioma pozostałymi zasadami dotyczącymi przetwarzania danych, o których mowa w art. 5 ust. 1) zgodnie z zasadą rozliczalności.

[9] W art. 24 ust. 1 przewidziano obowiązek, zgodnie z którym administrator danych ma wdrażać odpowiednie środki techniczne i organizacyjne, aby wykazać, że przetwarzanie odbywało się zgodnie z RODO.

4. Przejrzystość (o ile jest przestrzegana przez administratorów danych) uprawnia osoby, których dane dotyczą, do pociągania do odpowiedzialności administratorów lub podmiotów przetwarzających i do sprawowania kontroli nad swoimi danymi osobowymi, np. poprzez udzielenie lub wycofanie świadomej zgody i wykonywanie praw przysługujących osobom, których dane dotyczą[10]. Koncepcja przejrzystości w RODO skupia się w większym stopniu na użytkowniku niż na aspektach prawnych i jest realizowana za pomocą szczególnych wymogów praktycznych, które wiążą administratorów danych lub podmioty przetwarzające i są określone w wielu artykułach. Wymogi praktyczne (dotyczące informowania) wyszczególniono w art. 12–14 RODO. Jakość, dostępność i zrozumiałość informacji jest jednak tak samo ważna jak rzeczywista treść informacji dotyczących przejrzystości, którą należy udostępnić osobom, których dane dotyczą.

5. Ustanowione w RODO wymogi przejrzystości mają zastosowanie bez względu na podstawę prawną przetwarzania i na każdym etapie przetwarzania. Wynika to wyraźnie z art. 12, który stanowi, że przejrzystość należy zapewnić na następujących etapach cyklu przetwarzania danych:

- przed rozpoczęciem cyklu przetwarzania danych lub w chwili jego rozpoczęcia, tj. w momencie zbierania danych osobowych od osoby, której dane dotyczą, lub uzyskiwania ich w inny sposób;
- przez cały czas przetwarzania, tj. w momencie informowania osób, których dane dotyczą, o ich prawach; oraz
- w poszczególnych momentach przetwarzania, tj. kiedy występują naruszenia ochrony danych lub w przetwarzaniu zachodzą istotne zmiany.

Znaczenie przejrzystości

6. RODO nie zawiera definicji przejrzystości. Motyw 39 RODO zawiera informacje na temat znaczenia i skutków zasady przejrzystości w kontekście przetwarzania danych:

> „Dla osób fizycznych powinno być przejrzyste, że dotyczące ich dane osobowe są zbierane, wykorzystywane, przeglądane lub w inny sposób przetwarzane oraz w jakim stopniu te dane osobowe są lub będą przetwarzane. Zasada przejrzystości wymaga, by wszelkie informacje i wszelkie komunikaty związane z przetwarzaniem tych danych osobowych były łatwo dostępne i zrozumiałe oraz sformułowane jasnym i prostym językiem. Zasada ta dotyczy w szczególności informowania osób, których dane dotyczą, o tożsamości administratora i celach przetwarzania oraz innych informacji mających zapewnić rzetelność i przejrzystość przetwarzania

[10] Zob. np. opinia rzecznika generalnego Cruza Villalóna (9 lipca 2015 r.) w sprawie C-201/14 Bara, pkt 74: „ten wymóg informowania osób, których dotyczy przetwarzanie ich danych osobowych, który gwarantuje przejrzystość wszelkich czynności przetwarzania, jest tym ważniejszy, iż uzależnione jest od niego wykonywanie przez osoby zainteresowane ich prawa dostępu do przetwarzanych danych, przewidzianego w art. 12 dyrektywy 95/46, oraz ich prawa sprzeciwu wobec przetwarzania tych danych, zdefiniowanego w art. 14 tej dyrektywy".

w stosunku do osób, których sprawa dotyczy, a także prawa takich osób do uzyskania potwierdzenia i informacji o przetwarzanych danych osobowych ich dotyczących".

Elementy przejrzystości w świetle RODO

7. Artykuły, które mają największe znaczenie w zakresie przejrzystości w RODO, ponieważ mają zastosowanie do praw osób, których dane dotyczą, znajdują się w rozdziale III („Prawa osoby, której dane dotyczą"). W art. 12 ustanowiono ogólne zasady, które mają zastosowanie do: udzielania informacji osobom, których dane dotyczą (na podstawie art. 13–14); powiadamiania osób, których dane dotyczą, o wykonywaniu ich praw (na podstawie art. 15–22); oraz powiadamiania o naruszeniach ochrony danych (art. 34). W szczególności w art. 12 wymaga się, by dane informacje lub komunikacja były zgodne z następującymi zasadami:

- muszą być w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie (art. 12 ust. 1);
- należy używać jasnego i prostego języka (art. 12 ust. 1);
- wymóg jasnego i prostego języka ma szczególne znaczenie, jeżeli informacje są kierowane do dziecka (art. 12 ust. 1);
- informacje są udzielane na piśmie „lub w inny sposób, w tym w stosownych przypadkach – elektronicznie" (art. 12 ust. 1);
- jeżeli osoba, której dane dotyczą, tego zażąda, informacji można udzielić ustnie (art. 12 ust. 1); oraz
- informacje i komunikacja są zasadniczo wolne od opłat (art. 12 ust. 5).

Zwięzła, przejrzysta, zrozumiała i łatwo dostępna forma

8. Wymóg, zgodnie z którym podawanie informacji osobom, których dane dotyczą, i komunikacja z nimi odbywa się w „zwięzłej, przejrzystej, zrozumiałej i łatwo przystępnej formie", oznacza, że administratorzy danych powinni przekazywać informacje / komunikować się w sposób efektywny i zwięzły, tak aby nie przytłoczyć odbiorcy informacjami. Informacje te należy wyraźnie odróżnić od innych informacji niezwiązanych z prywatnością, np. postanowień umownych lub ogólnych warunków korzystania. W kontekście internetu zastosowanie warstwowego oświadczenia / warstwowej informacji o ochronie prywatności umożliwi osobie, której dane dotyczą, przejście do konkretnej części oświadczenia o ochronie prywatności / informacji o polityce prywatności, do której chce się natychmiast dostać, w związku z czym nie będzie musiała przewijać długiego tekstu w poszukiwaniu konkretnych kwestii.

9. Wymóg „zrozumiałości" informacji oznacza, że powinien ją zrozumieć przeciętny przedstawiciel grupy docelowych odbiorców. Zrozumiałość ma ścisły związek z wymogiem stosowania jasnego i prostego języka. Odpowiedzialny administrator danych będzie posiadał wiedzę na temat osób, o których zbiera informację, i będzie mógł ją wykorzystać, aby określić, jakie sformułowania będą najprawdopodobniej zrozumiałe dla odbiorców.

Przykładowo, administrator zbierający dane osobowe wysoko wykwalifikowanych specjalistów może założyć wyższy stopień zrozumienia odbiorców niż administrator, który zbiera dane osobowe dzieci. Jeżeli administratorzy nie mają pewności co do stopnia zrozumiałości i przejrzystości informacji oraz skuteczności interfejsów użytkownika / powiadomień / polityk itd., mogą zbadać te kwestie, np. wykorzystując mechanizmy takie jak panele użytkowników, testy czytelności, interakcje formalne i nieformalne oraz dialog z grupami branżowymi, grupami reprezentującymi konsumentów i organami regulacyjnymi, stosownie do przypadku.

10. Najważniejszym aspektem zasady przejrzystości, którą określono we wspomnianych przepisach, jest to, że osoba, której dane dotyczą, powinna zawsze być w stanie z wyprzedzeniem określić zakres i skutki przetwarzania i że nie powinna zostać później zaskoczona informacją, w jaki sposób wykorzystano jej dane osobowe. Jest to również ważny aspekt zasady rzetelności, o której mowa w art. 5 ust. 1 RODO, o czym świadczy związek tych przepisów z motywem 39, zgodnie z którym „[o]sobom fizycznym należy uświadomić ryzyka, zasady, zabezpieczenia i prawa związane z przetwarzaniem danych osobowych". Szczególnie w przypadku złożonego, technicznego lub niespodziewanego przetwarzania danych GR29 uważa, że poza zapewnieniem informacji wymaganych zgodnie z art. 13 i 14 (o których mowa w dalszej części niniejszych wytycznych) administratorzy powinni również oddzielnie i w sposób jednoznaczny wyjaśnić, jakie będą najważniejsze *skutki* przetwarzania: innymi słowy, jaki rzeczywisty wpływ na osobę, której dane dotyczą, będzie miało konkretne przetwarzanie opisane w oświadczeniu o ochronie prywatności / informacji o polityce prywatności. Zgodnie z zasadą rozliczalności i motywem 39 administratorzy danych powinni oceniać, czy istnieją szczególne zagrożenia dla osób fizycznych zaangażowanych w tego rodzaju przetwarzanie, o których należy powiadomić osoby, których dane dotyczą. Może to być pomocne w uzyskaniu ogólnego obrazu rodzajów przetwarzania, które mogą mieć największy wpływ na podstawowe prawa i wolności osób, których dane dotyczą, w związku z ochroną ich danych osobowych.

11. Element „łatwej dostępności" oznacza, że osoba, której dane dotyczą, nie powinna być zmuszona do wyszukiwania informacji; miejsce i sposób dostępu do informacji powinien od razu być dla niej oczywisty, co można zapewnić np. dzięki bezpośredniemu udzieleniu jej informacji, podaniu linków, wyraźnemu oznakowaniu takich informacji lub podaniu ich w formie odpowiedzi na pytanie sformułowanej w przystępny sposób (np. w internetowym warstwowym oświadczeniu o ochronie prywatności / warstwowej informacji o polityce prywatności, w FAQ, za pośrednictwem kontekstowych wyskakujących okien, które uruchamiają się podczas wypełniania internetowego formularza przez osobę, której dane dotyczą, lub – w interaktywnym kontekście cyfrowym – za pośrednictwem interfejsu chatbota itd. Mechanizmy te omówiono poniżej, w tym w pkt 33–40).

Przykład

Każda organizacja, która prowadzi stronę internetową, powinna opublikować na niej oświadczenie o ochronie prywatności / informację o polityce prywatności. Na każdej podstronie tej strony należy umieścić bezpośredni link do oświadczenia o ochronie

prywatności / informacji o polityce prywatności, używając powszechnie stosowanego hasła (np. „Ochrona prywatności", „Polityka ochrony prywatności" lub „Informacja o polityce prywatności"). Pozycjonowanie lub schematy kolorystyczne, które sprawiają, że tekst lub link są mniej widoczne lub trudniejsze do zlokalizowania na stronie internetowej, nie są uważane za łatwo dostępne.

W przypadku aplikacji niezbędne informacje należy udostępnić również z poziomu sklepu internetowego przed pobraniem. Łatwą dostępność informacji należy zapewnić również z poziomu aplikacji po jej zainstalowaniu. Jednym ze sposobów spełnienia tego wymogu jest zapewnienie, by informacja była zawsze dostępna najwyżej po dwóch „kliknięciach" (np. poprzez dodanie opcji „Ochrona prywatności" / „Ochrona danych osobowych" w menu aplikacji). Ponadto omawiane informacje dotyczące prywatności powinny być opracowane indywidualnie dla danej aplikacji; generyczna informacja o polityce ochrony prywatności stosowanej przez przedsiębiorstwo będące właścicielem lub dystrybutorem aplikacji jest niewystarczająca.

Jako najlepszą praktykę GR29 zaleca, by w momencie zbierania danych osobowych w środowisku online podawano link do oświadczenia o ochronie prywatności / informacji o polityce prywatności lub by udostępniano te informacje na tej samej stronie, na której zbiera się dane osobowe.

Jasny i prosty język

12. W przypadku informacji *pisemnych* (oraz gdy informacje pisemne są udzielane ustnie lub metodami dźwiękowo / audiowizualnymi, w tym osobom dotkniętym zaburzeniami widzenia) należy przestrzegać najlepszych praktyk w zakresie zrozumiałego stylu tekstu[11]. Podobny wymóg stylistyczny (dotyczący „prostego i zrozumiałego języka") był już wcześniej stosowany przez prawodawcę Unii[12] i został również wyraźnie wskazany w kontekście zgody w motywie 42 RODO[13]. Wymóg stosowania jasnego i prostego języka oznacza, że informacji należy udzielać w możliwie najprostszy sposób, bez stosowania złożonych struktur zdaniowych i językowych. Informacje powinny być konkretne i jednoznaczne; nie należy ich formułować przy pomocy pojęć abstrakcyjnych lub wieloznacznych ani pozostawiać dowolności interpretacji. Należy zwłaszcza jednoznacznie określić cele i podstawę prawną przetwarzania danych osobowych.

Przykłady złych praktyk

Poniższe zdania nie są wystarczająco jasne do celów przetwarzania:

- „Możemy wykorzystywać Twoje dane osobowe do opracowywania nowych usług" (nie wskazano wyraźnie, czym są „usługi", ani w jaki sposób dane pomogą ich w opracowaniu);
- „Możemy wykorzystywać Twoje dane osobowe do celów badawczych" (nie wskazano wyraźnie, o jakiego typu „badania" chodzi); oraz
- „Możemy wykorzystywać Twoje dane osobowe do oferowania spersonalizowanych usług" (nie wskazano wyraźnie, na czym polega „personalizacja").

Przykłady dobrych praktyk[14]

- „Będziemy przechowywać historię Twoich zakupów i wykorzystywać szczegółowe informacje na temat produktów, które kupiłeś w przeszłości, aby proponować Ci inne produkty, którymi naszym zdaniem możesz być zainteresowany" (wyraźnie wskazano, jakie rodzaje danych będą przetwarzane oraz że osoba, której dane dotyczą, będzie otrzymywać ukierunkowane reklamy produktów i że dane tej osoby będą wykorzystywane w tym celu);
- „Będziemy przechowywać i badać informacje na temat Twoich ostatnich wizyt na naszej stronie i sposobu, w jaki poruszasz się po różnych sekcjach naszej strony, do celów analitycznych, aby dowiedzieć się, w jaki sposób użytkownicy korzystają z naszej strony, i uczynić ją bardziej intuicyjną" (wyraźnie wskazano, jakie rodzaje danych będą przetwarzane, oraz rodzaj analizy, którą administrator ma zamiar przeprowadzać); oraz
- „Będziemy rejestrować, na które artykuły na naszej stronie kliknąłeś, i wykorzystamy te informacje do tworzenia na tej stronie reklam przeznaczonych dla Ciebie, które będą dopasowane do Twoich zainteresowań, zidentyfikowanych przez nas na podstawie przeczytanych przez Ciebie artykułów" (wyraźnie wskazano, co obejmuje personalizacja i w jaki sposób określono zainteresowania osoby, której dane dotyczą).

13. Należy również unikać takich wyrazów określających jak „może", „niektóre", „często" i „możliwe". Jeżeli administratorzy danych postanowią używać bardziej wieloznacznych sformułowań, zasada rozliczalności wymaga, aby byli w stanie wykazać, dlaczego nie można było uniknąć stosowania takich sformułowań i że nie wpływają one na rzetelność

[11] Zob. wytyczne Komisji Europejskiej pt. „Jak pisać zrozumiale" (2011), dostępne pod adresem: https://publications.europa.eu/en/publication-detail/-/publication/c2dab20c-0414-408d-87b5-dd3c6e5dd9a5.

[12] Art. 5 dyrektywy Rady 93/13/EWG z dnia 5 kwietnia 1993 r. w sprawie nieuczciwych warunków w umowach konsumenckich.

[13] Zgodnie z motywem 42 oświadczenie o wyrażeniu zgody przygotowane przez administratora powinno mieć zrozumiałą i łatwo dostępną formę, być sformułowane jasnym i prostym językiem i nie powinno zawierać nieuczciwych warunków.

[14] Wymóg przejrzystości funkcjonuje zupełnie niezależnie od obowiązku upewnienia się przez administratorów danych o istnieniu właściwej podstawy prawnej przetwarzania zgodnie z art. 6.

przetwarzania. Należy zadbać o właściwą strukturę akapitów i zdań, stosując wypunktowania i wcięcia w tekście, aby wskazać związki hierarchiczne. Należy używać strony czynnej, a nie biernej, oraz unikać zbyt wielu rzeczowników. Informacje podawane osobie, której dane dotyczą, nie powinny być napisane zbyt prawniczym, technicznym lub specjalistycznym językiem ani zawierać słów o takim charakterze. Jeżeli informacje są tłumaczone na język obcy, administrator danych powinien zapewnić, by wszystkie tłumaczenia były wierne oraz by frazeologia i składnia tekstów w języku obcym były zrozumiałe, tak by nie trzeba było rozszyfrowywać znaczenia przetłumaczonego tekstu lub dokonywać jego reinterpretacji. (Jeżeli administrator kieruje informacje[15] do osób, których dane dotyczą i które posługują się innym językiem lub innymi językami, należy zapewnić tłumaczenie w tym języku lub tych językach.)

Udzielanie informacji dzieciom i innym osobom wymagającym szczególnego traktowania

14. Jeżeli administrator danych kieruje informacje do dzieci[16] lub wie / powinien wiedzieć, że jego towary/usługi są często wykorzystywane przez dzieci (również w przypadku, gdy administrator opiera się na zgodzie udzielonej przez dziecko)[17], powinien zapewnić, by stosowane słownictwo oraz ton i styl wypowiedzi były właściwe i dobrze zrozumiałe dla dzieci, tak aby dziecko będące odbiorcą informacji wiedziało, że wiadomość/informacja jest skierowana do niego[18]. Użytecznym przykładem języka kierowanego głównie do dziecka jako alternatywy dla pierwotnego języka prawniczego jest Konwencja ONZ o prawach dziecka w języku przyjaznym dla dzieci („UN Convention on the Rights of the Child in Child Friendly Language")[19].

15. Zdaniem GR29 prawo do przejrzystości jest samodzielnym prawem, które ma zastosowanie w takim samym stopniu do dzieci, jak do dorosłych. GR29 podkreśla w szczególności, że dzieci jako osoby, których dane dotyczą, nie tracą swoich praw do przejrzystości tylko dlatego, że zgodę wyraziła lub zaaprobowała osoba posiadająca odpowiedzialność rodzicielską w sytuacji, do której zastosowanie ma art. 8 RODO. W wielu przypadkach osoba posiadająca odpowiedzialność rodzicielską wyraża lub aprobuje zgodę jednorazowo, ale dziecko (podobnie jak każda inna osoba, której dane dotyczą) ma stale prawo do przejrzystości przez cały okres trwania relacji z administratorem danych. Jest to zgodne z art. 13 Konwencji ONZ o prawach dziecka, który stanowi, że dziecko ma prawo do swobodnej wypowiedzi, w tym prawo poszukiwania, otrzymywania i przekazywania informacji oraz idei wszelkiego rodzaju[20]. Należy podkreślić, że co prawda w art. 8 przewidziano możliwość wyrażenia zgody w imieniu dziecka przed osiągnięciem przez nie odpowiedniego wieku[21], ale *nie przewidziano w nim* środków zapewnienia przejrzystości kierowanych do osoby posiadającej odpowiedzialność rodzicielską, która wyraża taką zgodę. Zgodnie z konkretnymi wzmiankami o kierowanych do dzieci środkach zapewnienia przejrzystości, o których mowa w art. 12 ust. 1 (oraz w motywach 38 i 58), administratorzy danych, którzy kierują informacje do dzieci albo wiadomo im, że z ich towarów lub usług korzystają często dzieci w wieku, w którym prawdopodobnie umieją czytać, mają w związku z tym obowiązek zapewnić, by wszelkie informacje i komunikaty były przekazywane w jasnym i prostym języku lub w formie, którą dzieci mogą łatwo zrozumieć. Aby uniknąć wątpliwości, GR29 uznaje jednak, że w przypadku bardzo małych dzieci lub dzieci będących w wieku, w którym prawdopodobnie nie umieją czytać, można również wdrożyć środki zapewnienia przejrzystości skierowane do osób posiadających odpowiedzialność rodzicielską, ponieważ w większości przypadków takie dzieci prawdopodobnie nie będą w stanie zrozumieć nawet najbardziej podstawowych wiadomości dotyczących przejrzystości, czy to pisemnych, czy też w innej formie.

16. Analogiczna sytuacja ma miejsce, gdy administratorowi danych jest wiadomo, że jego docelowymi klientami lub użytkownikami jego towarów lub usług są inni członkowie społeczeństwa wymagający szczególnego traktowania, w tym osoby niepełnosprawne lub osoby, które mogą mieć trudności z dostępem do informacji – wówczas administrator danych powinien uwzględnić ich trudności, oceniając możliwości wypełnienia przez niego obowiązków zapewnienia przejrzystości wobec osób, których dane dotyczą[22]. Dotyczy to konieczności dokonania przez administratora danych oceny prawdopodobnego poziomu zrozumienia przez grupę docelową, co zostało omówione powyżej w pkt 9.

Na piśmie lub w inny sposób

17. Zgodnie z art. 12 ust. 1 domyślną formą udzielania informacji lub komunikacji z osobami, których dane dotyczą, jest udzielanie informacji na piśmie[23]. (W art. 12 ust. 7 przewidziano również, że informacje można opatrzyć standardowymi znakami graficznymi; kwestię tę poruszono w sekcji poświęconej narzędziom wizualizacyjnym w pkt 49–53). W RODO przewidziano jednak możliwość korzystania z innych, nieokreślonych „środków", w tym

[15] Na przykład, jeżeli administrator prowadzi stronę internetową w danym języku lub oferuje opcje dla poszczególnych państw lub umożliwia płatność za towary i usługi w walucie danego państwa członkowskiego, może to wskazywać, że kieruje informacje do osób, których dane dotyczą, w konkretnym państwie członkowskim.

[16] W RODO nie zdefiniowano pojęcia „dziecka", jednak GR29 uznaje, że zgodnie z Konwencją ONZ o prawach dziecka, którą ratyfikowały wszystkie państwa członkowskie UE, dzieckiem jest osobą w wieku poniżej 18 lat.

[17] Tj. przez dziecko w wieku co najmniej 16 lat (albo – jeżeli zgodnie z art. 8 ust. 1 RODO państwa członkowskie przewidziały w swoim prawie, że granica wiekowa do celów udzielenia zgody na oferowanie świadczenia usług społeczeństwa informacyjnego przypada między 13. a 16. rokiem życia – przez dziecko, które przekroczyło granicę wiekową przewidzianą w prawie krajowym).

[18] W motywie 38 stwierdzono, że „Szczególnej ochrony danych osobowych wymagają dzieci, gdyż mogą one być mniej świadome ryzyka, konsekwencji, zabezpieczeń i praw przysługujących im w związku z przetwarzaniem danych osobowych". W motywie 58 stwierdzono, że „Zważywszy że dzieci zasługują na szczególną ochronę, wszelkie informacje i komunikaty – gdy przetwarzanie dotyczy dziecka – powinny być sformułowane tak jasnym i prostym językiem, by dziecko mogło je bez trudu zrozumieć".

[19] https://www.unicef.org/rightsite/files/uncrcchildfriendlylanguage.pdf

[20] Art. 13 Konwencji ONZ o prawach dziecka stanowi, że: „Dziecko będzie miało prawo do swobodnej wypowiedzi; prawo to ma zawierać swobodę poszukiwania, otrzymywania i przekazywania informacji oraz idei wszelkiego rodzaju, bez względu na granice, w formie ustnej, pisemnej bądź za pomocą druku, w formie artystycznej lub z wykorzystaniem każdego innego środka przekazu według wyboru dziecka".

[21] Zob. przypis 17 powyżej.

[22] Przykładowo w Konwencji o prawach osób niepełnosprawnych istnieje wymóg zapewnienia odpowiednich form pomocy i wsparcia dla osób niepełnosprawnych w celu zapewnienia im dostępu do informacji.

[23] W art. 12 ust. 1 pojawia się pojęcie „języka"; ponadto artykuł ten stanowi, że informacji udziela się na piśmie lub w inny sposób, w tym w stosownych przypadkach – elektronicznie.

drogi elektronicznej. Jeżeli chodzi o pisemne środki elektroniczne, GR29 uważa, że jeżeli administrator danych prowadzi stronę internetową (lub prowadzi całość lub część swojej działalności za pośrednictwem strony internetowej), GR29 zaleca stosowanie warstwowych oświadczeń o ochronie prywatności / warstwowych informacji o polityce prywatności, dzięki których osoby odwiedzające stronę internetową mogą zapoznać się z najbardziej interesującymi dla nich fragmentami danego oświadczenia o ochronie prywatności / informacji o polityce prywatności (więcej informacji na temat oświadczeń o ochronie prywatności / informacji o polityce prywatności znajduje się w pkt 35–37)[24]. Osoby, których dane dotyczą, powinny mieć jednak dostęp do wszystkich skierowanych do nich informacji również w jednym miejscu lub w ramach jednego dokumentu (elektronicznego lub papierowego), który powinien być łatwo dostępny dla takiej osoby, jeżeli zechce ona zapoznać się ze wszystkimi skierowanymi do niej informacjami. Należy podkreślić, że stosowanie warstwowej struktury nie ogranicza się wyłącznie do pisemnych środków elektronicznych stosowanych w celu udzielania informacji osobom, których dane dotyczą. Jak omówiono w pkt 35–36 i 38 poniżej, warstwową strukturę informacji udzielanych osobom, których dane dotyczą, można również zastosować przez połączenie kilku *metod* w celu zapewnienia przejrzystości przetwarzania.

18. Oczywiście stosowanie warstwowych oświadczeń o ochronie prywatności / warstwowych informacji o polityce prywatności w formie elektronicznej nie stanowi jedynego pisemnego środka elektronicznego, który mogą stosować administratorzy. Inne środki elektroniczne obejmują wyskakujące powiadomienia kontekstowe typu „just-in-time", powiadomienia za pomocą funkcji 3D Touch lub powiadomienia wyświetlające się po najechaniu kursorem oraz pulpity nawigacyjne prywatności. Niepisemne środki elektroniczne, które można wykorzystać *oprócz* warstwowego oświadczenia o ochronie prywatności / warstwowej informacji o polityce prywatności, mogą obejmować filmy wideo oraz powiadomienia na smartfon lub powiadomienia głosowe w technologii internetu rzeczy[25]. „Inne środki", które nie muszą być środkami elektronicznymi, mogą obejmować np. komiksy, infografiki lub schematy blokowe. Jeżeli informacje dotyczące przejrzystości są kierowane do dzieci, administratorzy powinni rozważyć, jakie rodzaje środków mogą być szczególnie przystępne dla dzieci (m.in. komiksy/kreskówki, piktogramy, animacje itd.).

19. Najważniejsze jest, aby wybrane metody udzielania informacji były dostosowane do konkretnej sytuacji, tj. do sposobu komunikacji między administratorem danych a osobą, której dane dotyczą, lub sposobu zbierania informacji odnoszących się do tej osoby. Przykładowo udzielanie informacji wyłącznie w pisemnym formacie elektronicznym, np. w formie internetowego oświadczenia o ochronie prywatności / informacji o polityce prywatności, może być niewłaściwe/niepraktyczne, gdy urządzenie rejestrujące dane osobowe nie ma ekranu (np. urządzenia połączone za pośrednictwem internetu rzeczy / urządzenia inteligentne), na którym mogą być wyświetlane strony internetowe / takie

[24] GR29 uznała już korzyści wynikające z warstwowej struktury informacji w opinii 10/2004 w sprawie bardziej ujednoliconych przepisów dotyczących informacji i w opinii 02/2013 w sprawie aplikacji na urządzenia inteligentne.

[25] Powyższe przykłady środków elektronicznych mają jedynie charakter orientacyjny, a administratorzy danych mogą opracować nowe innowacyjne metody, aby zapewnić zgodność z art. 12.

pisemne informacje. W takich przypadkach należy rozważyć zastosowanie odpowiednich *dodatkowych* środków alternatywnych, np. umieszczenie oświadczenia o ochronie prywatności / informacji o polityce prywatności w papierowych instrukcjach lub podanie adresu URL strony internetowej (tzn. jej konkretnej podstrony), pod którym można znaleźć internetowe oświadczenie o ochronie prywatności / informację o polityce prywatności, w papierowej instrukcji lub na opakowaniu. Można również dodatkowo przekazać informacje w formie dźwiękowej (ustnej), jeżeli urządzenie bez ekranu może odtwarzać dźwięk. GR29 sformułowała wcześniej zalecenia dotyczące przejrzystości i przekazywania informacji osobom, których dane dotyczą, w opinii na temat ostatnich postępów w dziedzinie internetu rzeczy[26] (np. stosowania kodów QR wydrukowanych na obiektach w technologii internetu rzeczy, tak aby po zeskanowaniu kodu QR wyświetliły się wymagane informacje dotyczące przejrzystości). Zalecenia te mają zastosowanie również w zakresie RODO.

…informacji można udzielić ustnie…

20. W art. 12 ust. 1 przewidziano w szczególności, że na żądanie osoby, której dane dotyczą, informacji można udzielić ustnie, o ile innymi sposobami potwierdzi się jej tożsamość. Innymi słowy, sposób potwierdzenia tożsamości nie powinien opierać się wyłącznie na zapewnieniu danej osoby, że jest ona osobą o danym imieniu i nazwisku, oraz powinien umożliwiać administratorowi weryfikację tożsamości osoby, której dane dotyczą, dającą wystarczającą pewność. Wymóg weryfikacji tożsamości osoby, której dane dotyczą, przed przekazaniem informacji ustnie, ma zastosowanie tylko do tych informacji, które dotyczą wykonywania przez osobę, której dane dotyczą, jej praw przewidzianych w art. 15–22 i 34. Ten warunek wstępny dotyczący przekazywania informacji ustnie nie może mieć zastosowania do przekazywania ogólnych informacji na temat ochrony prywatności, o których mowa w art. 13 i 14, ponieważ informacje wymagane na podstawie art. 13 i 14 muszą być udostępniane również *przyszłym* użytkownikom/klientom (których tożsamości administrator danych nie jest w stanie zweryfikować). W związku z tym informacje, których należy udzielić na podstawie art. 13 i 14, mogą zostać przekazane ustnie bez konieczności potwierdzenia przez administratora tożsamości osoby, której dane dotyczą.

21. Ustne udzielanie informacji, o których mowa w art. 13 i 14, niekoniecznie oznacza udzielenie informacji ustnie w formie bezpośredniego kontaktu z daną osobą (np. osobiście lub telefonicznie). Poza środkami pisemnymi można zapewnić automatyczne przekazywanie ustnych informacji. Taka sytuacja może mieć miejsce np. w kontekście osób słabowidzących, gdy kontaktują się one z dostawcami usług społeczeństwa informacyjnego, lub w kontekście urządzeń inteligentnych bez ekranów, o których wspomniano powyżej w pkt 19. GR29 jest zdania, że jeżeli administrator danych postanowi ustnie przekazać informacje osobie, której dane dotyczą, lub jeżeli osoba, której dane dotyczą, zażąda ustnego udzielenia informacji lub ustnej komunikacji, administrator danych powinien umożliwić osobie, której dane dotyczą, ponowne odsłuchanie nagranych

[26] Opinia GR29 8/2014 przyjęta w dniu 16 września 2014 r.

wiadomości. Jest to konieczne, jeżeli żądanie ustnego udzielenia informacji dotyczy osób słabowidzących, których dane dotyczą, lub innych osób, których dane dotyczą, mających problemy z dostępem do informacji w formie pisemnej lub z ich zrozumieniem. Administrator danych powinien również upewnić się, że prowadzona jest dokumentacja w odniesieniu do poniższych elementów i że może ją przedstawić (do celów spełnienia wymogu rozliczalności): (i) wniosek o ustne przekazanie informacji, (ii) metoda, którą zweryfikowano tożsamość osoby, której dane dotyczą (w stosownych przypadkach – zob. pkt 20 powyżej) oraz (iii) fakt, że informacje zostały przekazane osobie, której dane dotyczą.

Wolne od opłat

22. Zgodnie z art. 12 ust. 5[27] administratorzy danych zasadniczo nie mogą pobierać od osób, których dane dotyczą, opłat za przekazywanie informacji udzielanych na podstawie art. 13 i 14 ani za komunikację i działania podejmowane na podstawie art. 15–22 (dotyczących praw osób, których dane dotyczą) i 34 (dotyczącego zawiadamiania osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych)[28]. Ten aspekt przejrzystości oznacza również, że nie wolno uzależniać przekazania informacji udzielanych zgodnie z wymogami przejrzystości od dokonania transakcji finansowej, np. zapłaty za usługi lub towary bądź ich zakupu[29].

Informacje udzielane osobie, której dane dotyczą – art. 13 i 14

Treść

23. W RODO wymieniono kategorie informacji, których należy udzielić osobie, której dane dotyczą, w związku z przetwarzaniem danych osobowych tej osoby, bez względu na to, czy zostały zebrane od osoby, której dane dotyczą (art. 13), czy też pozyskane z innego źródła (art. 14). W **tabeli w załączniku** do niniejszych wytycznych podsumowano kategorie informacji, których należy udzielić na podstawie art. 13 i 14. W tabeli opisano również charakter, zakres i treść tych wymogów. Należy wyjaśnić, że GR29 reprezentuje stanowisko, iż status informacji udzielanych na podstawie ust. 1 i 2 odpowiednio w art. 13 oraz w art. 14 jest taki sam. Wszystkie informacje, o których mowa w tych ustępach, są równie ważne i muszą zostać udzielone osobie, której dane dotyczą.

[27] Zgodnie z tym artykułem „informacje podawane na mocy art. 13 i 14 oraz komunikacja i działania podejmowane na mocy art. 15–22 i 34 są wolne od opłat".

[28] Zgodnie z art. 12 ust. 5 administrator może jednak pobrać rozsądną opłatę, jeżeli np. żądanie osoby, której dane dotyczą, względem informacji udzielanych na podstawie art. 13 i 14 lub praw przewidzianych w art. 15–22 lub 34 jest ewidentnie nieuzasadnione lub nadmierne. (Oddzielnie administrator może – w związku z prawem dostępu przewidzianym w art. 15 ust. 3 – pobrać rozsądną opłatę, uwzględniając administracyjne koszty kolejnych kopii danych osobowych sporządzanych na wniosek osoby, której dane dotyczą).

[29] Na przykład, jeżeli dane osobowe osoby, której dane dotyczą, są zbierane w związku z zakupem, informacje, które należy podać na podstawie art. 13, powinny zostać przekazane przed dokonaniem płatności i w momencie zbierania informacji, a nie po zawarciu transakcji. Jeżeli jednak osobie, której dane dotyczą, oferowane są nieodpłatne usługi, wówczas informacje przewidziane w art. 13 również muszą być udzielone przed rejestracją, a nie po niej, ponieważ w art. 13 ust. 1 przewidziano wymóg podania informacji „podczas pozyskiwania danych osobowych".

Odpowiednie środki

24. Ważna jest nie tylko treść, ale również forma i sposób, w który informacje udzielane na podstawie art. 13 i 14 powinny być przekazane osobie, której dane dotyczą. Powiadomienie zawierające takie informacje zwane jest często powiadomieniem o ochronie danych, informacją o polityce prywatności, polityką ochrony prywatności, oświadczeniem o ochronie prywatności lub informacją o rzetelnym przetwarzaniu. W RODO nie określono formatu lub sposobu udzielania takich informacji osobie, której dane dotyczą, ale stwierdzono w nim wyraźnie, że administrator danych ma obowiązek podjąć „odpowiednie środki" w związku z udzielaniem wymaganych informacji do celów zapewnienia przejrzystości. Oznacza to, że wybierając właściwy sposób i format udzielania informacji, administrator danych powinien uwzględnić wszelkie okoliczności zbierania i przetwarzania danych. W szczególności należy ocenić odpowiednie środki pod kątem doświadczenia użytkownika produktu/usługi. Oznacza to uwzględnienie urządzenia, z którego korzysta użytkownik (w stosownych przypadkach), charakterystyki interfejsów użytkownika / komunikacji z administratorem danych („zestaw interakcji" użytkownika) oraz ograniczeń, które wynikają z tych czynników. Jak wskazano powyżej w pkt 17, GR29 zaleca, by korzystano z warstwowego internetowego oświadczenia o ochronie prywatności / warstwowej informacji o polityce prywatności, jeżeli administrator danych działa w internecie.

25. Aby ułatwić określenie najwłaściwszych sposobów udzielania informacji, zanim zostaną zastosowane w praktyce, administratorzy danych mogą sprawdzić różne sposoby w drodze testowania przez użytkownika (np. badania typu *hall test* lub inne standardowe testy czytelności lub przystępności), aby uzyskać informacje zwrotne od użytkownika na temat przystępności, zrozumienia i łatwości stosowania proponowanego środka. (Zob. również powyższe szczegółowe uwagi na temat innych mechanizmów przeprowadzania testów przez użytkownika w pkt 9). Udokumentowanie tego podejścia powinno ponadto pomóc administratorom danych w wywiązaniu się z ich obowiązków w zakresie rozliczalności, ponieważ będą mogli w ten sposób wykazać, dlaczego narzędzie/podejście wybrane do podania informacji jest najwłaściwszym w danych okolicznościach.

Czas podawania informacji

26. W art. 13 i 14 określono informacje, których należy udzielić osobie, której dane dotyczą, na początku cyklu przetwarzania[30]. Art. 13 ma zastosowanie do scenariusza, w którym dane zbiera się od osoby, której dane dotyczą. Obejmuje dane osobowe, które:

[30] Zgodnie z zasadami rzetelności i ograniczenia celu organizacja, która pozyskuje dane osobowe od osoby, której dane dotyczą, zawsze powinna określić cele przetwarzania danych w momencie ich zbierania. Jeżeli jednym z takich celów jest tworzenie implikowanych danych osobowych, osoba, której dane dotyczą, zawsze musi zostać poinformowana o zamierzonym celu tworzenia i dalszego przetwarzania takich implikowanych danych oraz kategorii przetwarzanych implikowanych danych w momencie zbierania danych lub przed dalszym przetwarzaniem do nowego celu zgodnie z art. 13 ust. 3 lub art. 14 ust. 4.

- osoba, której dane dotyczą, świadomie przekazuje administratorowi danych (np. wypełniając formularz internetowy); lub
- administrator danych pozyskuje od osoby, której dane dotyczą, w drodze obserwacji (np. przy zastosowaniu automatycznych rejestratorów danych lub oprogramowania rejestrującego dane, np. kamer, urządzeń sieciowych, śledzenia sieci Wi-Fi, RFID lub innych rodzajów sensorów).

Art. 14 ma zastosowanie do scenariusza, w którym danych nie pozyskano od osoby, której dotyczą. Obejmują one dane osobowe, które administrator danych pozyskał ze źródeł takich jak:

- zewnętrzni administratorzy danych;
- źródła dostępne publicznie;
- pośrednicy danych; lub
- inne osoby, których dane dotyczą.

27. Jeżeli chodzi o czas udzielania tych informacji, ich udzielenie w odpowiednim czasie stanowi ważny element wykonania obowiązku zapewnienia przejrzystości i obowiązku rzetelnego przetwarzania danych. Jeżeli zastosowanie ma art. 13, informacje przewidziane w art. 13 ust. 1 muszą być podawane „podczas pozyskiwania danych osobowych". W przypadku danych osobowych pozyskiwanych pośrednio na podstawie art. 14, terminy, w których należy udzielić wymaganych informacji osobie, której dane dotyczą, określono w art. 14 ust. 3 lit. a)–c):

- zgodnie z ogólnym wymogiem informacje należy przekazać w „rozsądnym terminie" po pozyskaniu danych osobowych, a najpóźniej w ciągu miesiąca, „mając na uwadze konkretne okoliczności przetwarzania danych osobowych" (art. 14 ust. 3 lit. a));

- ogólny termin jednego miesiąca, o którym mowa w art. 14 ust. 3 lit. a), może zostać skrócony na podstawie art. 14 ust. 3 lit. b)[31], jeżeli dane są wykorzystywane do komunikacji z osobą, której dane dotyczą. Wówczas informacji należy udzielić najpóźniej przy pierwszej komunikacji z osobą, której dane dotyczą. Jeżeli pierwsza komunikacja następuje przed upływem terminu jednego miesiąca po uzyskaniu danych osobowych, wówczas informacji należy udzielić *najpóźniej* przy pierwszej komunikacji z osobą, której dane dotyczą, niezależnie od tego, że termin jednego miesiąca od chwili pozyskania danych nie upłynął. Jeżeli pierwsza komunikacja z osobą, której dane dotyczą, następuje po ponad jednym miesiącu od uzyskania danych osobowych, wówczas zastosowanie ma w dalszym ciągu art. 14 ust. 3 lit. a), tj. informacje udzielane na podstawie art. 14 muszą zostać przekazane osobie, której dane dotyczą, najpóźniej w ciągu jednego miesiąca od ich uzyskania;

- ogólny termin jednego miesiąca[32], o którym mowa w art. 14 ust. 3 lit. a), może zostać skrócony również na podstawie art. 14 ust. 3 lit. c), który ma zastosowanie, jeżeli planuje się ujawnić dane innemu odbiorcy (bez względu na to, czy jest on osobą trzecią)[33]. W takim przypadku informacji należy udzielić najpóźniej przy pierwszym ujawnieniu. Jeżeli wówczas pierwsze ujawnienie następuje przed upływem terminu jednego miesiąca, wówczas informacji należy udzielić *najpóźniej* przy pierwszym ujawnieniu, chociaż termin jednego miesiąca od chwili pozyskania danych nie upłynął. Podobnie do stanowiska, o którym mowa w art. 14 ust. 3 lit. b), jeżeli dane osobowe zostaną ujawnione później niż w ciągu jednego miesiąca od uzyskania danych osobowych, wówczas zastosowanie ma ponownie art. 14 ust. 3 lit. a), tj. informacje udzielane na podstawie art. 14 muszą zostać przekazane osobie, której dane dotyczą, najpóźniej w ciągu jednego miesiąca od ich pozyskania.

28. W związku z tym w każdym przypadku maksymalny termin, w którym należy udzielić informacji, o których mowa w art. 14, osobie, której dane dotyczą, wynosi jeden miesiąc. Zasady rzetelności i rozliczalności w ramach RODO wymagają jednak, aby podejmując decyzję o tym, w którym momencie udzielić informacji przewidzianych w art. 14, administratorzy danych zawsze brali pod uwagę rozsądne oczekiwania osób, których dane dotyczą, potencjalny wpływ przetwarzania na te osoby i ich zdolność do wykonywania praw w związku z tym przetwarzaniem. Zasada rozliczalności wymaga, aby administratorzy wykazywali logikę, na której opierają swoje decyzje, i uzasadniali, dlaczego informacje podano w konkretnym czasie. W praktyce spełnienie tych wymogów może być trudne, jeżeli informacji udziela się „w ostatniej chwili". W tym względzie w motywie 39 przewidziano m.in., że osobom, których dane dotyczą „należy uświadomić ryzyka, zasady, zabezpieczenia i prawa związane z przetwarzaniem danych osobowych oraz sposoby wykonywania praw przysługujących im w związku z takim przetwarzaniem". W motywie 60 odniesiono się również do wymogu, zgodnie z którym osoba, której dane dotyczą, musi być informowana o prowadzeniu operacji przetwarzania i o jej celach w kontekście zasad rzetelnego i przejrzystego przetwarzania. W świetle powyższego GR29 jest zdania, że w każdym przypadku, gdy jest to możliwe, administratorzy danych powinni – zgodnie z zasadą rzetelności – udzielać informacji osobom, których dane dotyczą, z dużym wyprzedzeniem w stosunku do określonych w prawie terminów. Dalsze uwagi na temat odpowiednich okresów między powiadomieniem osób, których dane dotyczą, o operacjach

[31] Użycie sformułowania „jeżeli dane osobowe mają być stosowane do [...]" w art. 14 ust. 3 lit. b) wskazuje na uszczegółowienie ogólnego stanowiska dotyczącego maksymalnego terminu, który ustalono w art. 14 ust. 3 lit. a), ale nie zastępuje tego stanowiska.

[32] Użycie sformułowania „jeżeli planuje się ujawnić dane osobowe innemu odbiorcy" w art. 14 ust. 3 lit. c) również wskazuje na uszczegółowienie ogólnego stanowiska dotyczącego maksymalnego terminu, który ustalono w art. 14 ust. 3 lit. a), ale nie zastępuje tego stanowiska.

[33] W art. 4 pkt 9 znajduje się definicja „odbiorcy", zgodnie z którą odbiorca, któremu ujawniane są dane osobowe, nie musi być stroną trzecią. W związku z tym odbiorcą może być administrator danych, współadministrator lub podmiot przetwarzający.

przetwarzania a rzeczywistym przeprowadzeniem takich operacji przetwarzania zamieszczono w pkt 30–31 i 48.

Zmiany w informacjach, o których mowa w art. 13 i 14

29. Rozliczalność w zakresie przejrzystości ma zastosowanie nie tylko w chwili zbierania danych osobowych, ale przez cały czas przetwarzania, bez względu na przekazywane informacje lub komunikację. Ma to miejsce np. przy zmianie treści dotychczasowych oświadczeń o ochronie prywatności / informacji o polityce prywatności. Administrator powinien przestrzegać tych samych zasad, zarówno gdy przekazuje pierwsze oświadczenie o ochronie prywatności / informację o polityce prywatności, jak i gdy powiadamia o wszelkich istotnych lub dużych zmianach w tym oświadczeniu / tej informacji. Czynniki, które administratorzy powinni uwzględnić przy ocenie, czym jest istotna lub duża zmiana, obejmują wpływ na osoby, których dane dotyczą (w tym ich zdolność do wykonywania swoich praw), oraz na ile zmiana będzie niespodziewana lub zaskakująca dla osób, których dane dotyczą. Osoby, których dane dotyczą, zawsze powinny być informowane m.in. o następujących zmianach w oświadczeniu o ochronie prywatności / informacji o polityce prywatności: zmiana celu przetwarzania; zmiana tożsamości administratora; zmiana sposobu, w jaki osoby, których dane dotyczą, mogą wykonywać swoje prawa w związku z przetwarzaniem. Przykłady zmian w oświadczeniu o ochronie prywatności / informacji o polityce prywatności, które – zdaniem GR29 – nie są istotne ani duże, obejmują poprawę literówek lub błędów stylistycznych/gramatycznych. Ponieważ większość klientów lub użytkowników jedynie pobieżnie czyta komunikaty na temat zmian w oświadczeniach o ochronie prywatności / informacjach o polityce prywatności, administrator powinien zastosować wszelkie niezbędne środki, aby zapewnić komunikowanie tych zmian w taki sposób, aby większość odbiorców rzeczywiście je dostrzegła. Oznacza to np. że komunikat w sprawie zmian powinien być zawsze przekazywany za pośrednictwem odpowiedniego środka (np. pocztą elektroniczną, listem, w wyskakującym oknie na stronie internetowej lub w inny sposób, który rzeczywiście zwróci uwagę na zmiany) specjalnie poświęconego tym zmianom (a nie np. razem z treściami z zakresu marketingu bezpośredniego), przy czym komunikat musi również spełniać wymogi przewidziane w art. 12, tj. zostać sporządzony w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem. Zamieszczenie w oświadczeniu o ochronie prywatności / informacji o polityce prywatności zalecenia dla osoby, której dane dotyczą, aby regularnie sprawdzała oświadczenie o ochronie prywatności / informację o polityce prywatności pod kątem zmian lub aktualizacji, uznaje się nie tylko za niewystarczające, ale również za nierzetelne w kontekście art. 5 ust. 1 lit. a). Dalsze wskazówki dotyczące terminów powiadamiania o zmianach osób, których dane dotyczą, zostały zamieszczone poniżej w pkt 30–31.

Terminy powiadamiania o zmianach w informacjach, o których mowa w art. 13 i 14

30. W RODO nie poruszono kwestii wymogów czasowych (ani metod), które mają zastosowanie do powiadamiania o zmianach w informacjach, których wcześniej udzielono osobie, której dane dotyczą, na podstawie art. 13 lub 14 (z wyjątkiem zamierzonego dalszego celu przetwarzania – w takim przypadku informacji na temat takiego dalszego celu

należy udzielić przed rozpoczęciem dalszego przetwarzania, co wynika z art. 13 ust. 3 i art. 14 ust. 4 – zob. pkt 45 poniżej). Jak jednak wspomniano powyżej w kontekście terminów podawania informacji określonych w art. 14, administrator danych również w tym wypadku musi przestrzegać zasad rzetelności i rozliczalności w zakresie wszelkich rozsądnych oczekiwań osoby, której dane dotyczą, lub potencjalnego wpływu tych zmian na osobę, której dane dotyczą. Jeżeli zmiana w informacjach wskazuje na istotną zmianę charakteru przetwarzania (np. rozszerzenie kategorii odbiorców lub rozpoczęcie przekazywanie danych do państw trzecich) lub zmianę, która nie musi być istotna w kontekście operacji przetwarzania, ale może mieć znaczenie dla osoby, której dane dotyczą, i wpływać na nią, wówczas takie informacje należy udostępnić osobie, której dane dotyczą, z dużym wyprzedzeniem w stosunku do wejścia zmiany w życie, a metoda zastosowana do zawiadomienia o tych zmianach osoby, której dane dotyczą, powinna zapewniać jasność i skuteczność. Celem powyższego jest zapewnienie, by osoba, której dane dotyczą, nie „przegapiła" zmiany i by zapewnić jej rozsądny czas na (a) rozważenie charakteru i wpływu zmiany i (b) wykonanie swoich praw na mocy RODO w związku ze zmianą (np. wycofanie zgody lub wniesienie sprzeciwu wobec przetwarzania).

31. Administratorzy danych powinni ostrożnie rozważyć okoliczności i kontekst każdej sytuacji, w której konieczna jest aktualizacja informacji dotyczących przejrzystości, w tym potencjalny wpływ zmian na osobę, której dane dotyczą, i sposób wykorzystany do powiadomienia o zmianach, oraz powinni być w stanie wykazać, w jaki sposób odstęp czasowy między powiadomieniem o zmianach a wejściem zmian w życie spełnia zasadę rzetelności względem osoby, której dane dotyczą. Ponadto GR29 jest zdania, że powiadamiając o takich zmianach osoby, których dane dotyczą, administrator danych powinien również wyjaśnić – zgodnie z zasadą rzetelności – jaki będzie prawdopodobny wpływ tych zmian na osoby, których dane dotyczą. Spełnienie wymogów przejrzystości nie może jednak kamuflować sytuacji, w której zmiany w przetwarzaniu są tak istotne, że charakter przetwarzania zmienia się całkowicie względem stanu poprzedniego. GR29 podkreśla, że wszystkie pozostałe zasady określone w RODO, w tym te związane z niewłaściwym dalszym przetwarzaniem, mają w dalszym ciągu zastosowanie, bez względu na konieczność wypełnienia obowiązków zapewnienia przejrzystości.

32. Ponadto nawet jeżeli informacje dotyczące przejrzystości (np. zawarte w oświadczeniu o ochronie prywatności / informacji o polityce prywatności) nie zmienią się w istotnym stopniu, istnieje prawdopodobieństwo, że osoby, których dane dotyczą i które korzystały z danej usług przez dłuższy czas, nie będą pamiętać, jakich informacji im udzielono na początku na podstawie art. 13 lub 14. GR29 zaleca, by administratorzy ułatwili osobom, których dane dotyczą, dalszy łatwy dostęp do informacji, aby mogły one ponownie się zapoznać z zakresem przetwarzania danych. Zgodnie z zasadą rozliczalności administratorzy powinni również rozważyć, czy i w jakich odstępach czasu powinni przesyłać osobom, których dane dotyczą, przypomnienia o istnieniu oświadczenia o ochronie prywatności / informacji o polityce prywatności i o miejscu, w którym mogą je znaleźć.

Tryb i format udzielania informacji

33. Zarówno w art. 13, jak i w art. 14 przewidziano obowiązek, zgodnie z którym administrator danych „podaje jej [osobie, której dane dotyczą] wszystkie następujące informacje (...)". Słowo „podaje" ma tutaj kluczowe znaczenie. Oznacza ono, że administrator danych musi czynnie podjąć działania w celu udzielenia osobie, której dane dotyczą, przedmiotowych informacji lub czynnie skierować ją do miejsca, w którym znajdują się te informacje (np. podając bezpośredni link, zachęcając do skorzystania z kodu QR itd.). Osoba, której dane dotyczą, nie powinna być zmuszona do czynnego szukania informacji, o których mowa we wspomnianych artykułach, wśród innych informacji, takich jak regulamin korzystania ze strony internetowej lub z aplikacji. Kwestię tę zilustrowano przykładem w pkt 11. Jak wskazano w pkt 17 powyżej, GR29 zaleca, by wszystkie informacje skierowane do osoby, której dane dotyczą, były dla niej również dostępne w jednym miejscu lub w ramach jednego dokumentu (np. elektronicznego na stronie internetowej lub papierowego), który powinien być łatwo dostępny na wypadek, gdyby osoba ta chciała zapoznać się z całością informacji.

34. W RODO istnieje pewien kontrast między, z jednej strony, wymogami przekazania osobom, których dane dotyczą, wyczerpujących informacji wymaganych na podstawie RODO, a z drugiej strony wymogami przekazania tych informacji w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie. Mając na uwadze fundamentalne zasady rozliczalności i rzetelności, administratorzy muszą samodzielnie przeanalizować charakter, okoliczności, zakres i kontekst prowadzonego przez nich przetwarzania danych osobowych oraz postanowić – w ramach wymogów prawnych ustanowionych w RODO i po uwzględnieniu zaleceń wskazanych w niniejszych wytycznych, w szczególności w pkt 36 poniżej – które z wymaganych informacji potraktować priorytetowo oraz jakie są właściwe poziomy szczegółowości i metody przekazywania informacji.

Warstwowe podejście w otoczeniu cyfrowym i warstwowe oświadczenia o ochronie prywatności / warstwowe informacje o polityce prywatności

35. W kontekście cyfrowym, biorąc pod uwagę ilość informacji, których należy udzielić osobie, której dane dotyczą, administratorzy danych mogą przyjąć warstwowe podejście, jeżeli chcą połączyć różne metody w celu zapewnienia przejrzystości. GR29 zaleca w szczególności, aby korzystano z warstwowych oświadczeń o ochronie prywatności / warstwowych informacji o polityce prywatności w celu odsyłania do różnych kategorii informacji, które należy podać osobie, której dane dotyczą, zamiast wyświetlać na ekranie wszystkie te informacje w formie ciągłego tekstu. Dzięki temu można uniknąć przeładowania informacyjnego. Warstwowe oświadczenia o ochronie prywatności / warstwowe informacje o polityce prywatności mogą pomóc zrównoważyć kwestie kompletności i zrozumienia, w szczególności dzięki umożliwieniu użytkownikom bezpośredniego przejścia do tej sekcji oświadczenia/informacji, którą chcą przeczytać. Należy podkreślić, że warstwowe oświadczenia o ochronie prywatności / warstwowe

informacje o polityce prywatności nie są zwykłymi podstronami, które wymagają kilku kliknięć, aby dotrzeć do danej informacji. Struktura i wygląd pierwszej warstwy oświadczenia o ochronie prywatności / informacji o polityce prywatności powinny dawać osobie, której dane dotyczą, jasny obraz, jakie informacje są dostępne na temat przetwarzania jej danych osobowych, oraz gdzie i w jaki sposób może znaleźć te szczegółowe informacje w warstwach oświadczenia o ochronie prywatności / informacji o polityce prywatności. Ważne jest również, aby informacje zawarte w poszczególnych warstwach informacji były ze sobą spójne i by nie znajdowały się tam sprzeczne informacje.

36. Jeżeli chodzi o treści podawane w ramach pierwszego sposobu, z którego korzysta administrator w celu przekazania informacji osobom, których dane dotyczą, w ramach warstwowego podejścia (innymi słowy – głównego sposobu, w który administrator po raz pierwszy wchodzi w interakcję z osobą, której dane dotyczą) lub treści zawarte w pierwszej warstwie oświadczenia o ochronie prywatności / informacji o polityce prywatności, GR29 zaleca, by ta pierwsza warstwa lub pierwszy sposób obejmowały szczegółowe informacje na temat celów przetwarzania, tożsamości administratora i opisu praw osoby, której dane dotyczą. (Ponadto na te informacje należy bezpośrednio zwrócić uwagę osoby, której dane dotyczą, w momencie pozyskiwania danych osobowych, np. wyświetlać je w momencie, kiedy osoba, której dane dotyczą, wypełnia formularz online.) Znaczenie podawania tych informacji z góry jest szczególnie podkreślone w motywie 39[34]. Chociaż administratorzy muszą być w stanie wykazać rozliczalność co do tego, jakie dalsze informacje postanowili traktować priorytetowo, GR29 uważa, że – zgodnie z zasadą rzetelności – obok informacji wskazanych powyżej w niniejszym punkcie, pierwsza warstwa / pierwszy sposób powinien również zawierać informacje na temat przetwarzania, które ma największy wpływ na osobę, której dane dotyczą, oraz przetwarzania, które może zaskoczyć taką osobę. W związku z tym osoba, której dane dotyczą, powinna być w stanie zrozumieć na podstawie informacji zawartych w pierwszej warstwie / pierwszym sposobie, jakie konsekwencje pociągnie za sobą dla niej to przetwarzanie (zob. również powyżej pkt 10).

37. W kontekście cyfrowym poza zapewnieniem warstwowego internetowego oświadczenia o ochronie prywatności / warstwowej informacji o polityce prywatności administrator danych może również postanowić, że zastosuje *dodatkowe* narzędzia do celów zapewnienia przejrzystości (zob. dalsze przykłady przeanalizowane poniżej), które komunikują poszczególnym osobom, których dane dotyczą, informacje specjalnie dostosowane do ich sytuacji oraz do towarów/usług, z których korzystają. Należy jednak podkreślić, że chociaż GR29 zaleca stosowanie warstwowych internetowych oświadczeń o ochronie prywatności /warstwowych informacji o polityce prywatności, niniejsze zalecenie nie wyklucza możliwości opracowania i stosowania innych innowacyjnych metod zapewniających przestrzeganie wymogów w zakresie przejrzystości.

[34] W odniesieniu do zasady przejrzystości motyw 39 stanowi, że „zasada ta dotyczy w szczególności informowania osób, których dane dotyczą, o tożsamości administratora i celach przetwarzania danych oraz innych informacji mających zapewnić rzetelność i przejrzystość przetwarzania w stosunku do osób, których sprawa dotyczy, a także prawa takich osób do uzyskania potwierdzenia i informacji o przetwarzanych danych osobowych ich dotyczących".

Warstwowe podejście w otoczeniu innym niż cyfrowe

38. Warstwowe podejście do udzielania informacji dotyczących przejrzystości osobom, których dane dotyczą, można zastosować również w kontekście innym niż internetowy/cyfrowy (np. w kontaktach osobistych lub w rozmowie telefonicznej), gdzie administratorzy danych mogą zastosować różne sposoby w celu ułatwienia podawania informacji. (Zob. również pkt 33–37 i 39–40 w odniesieniu do różnych sposobów podawania informacji.) Nie należy mylić tego pojęcia z odrębną kwestią warstwowych oświadczeń o ochronie prywatności / warstwowych informacji o polityce prywatności. Niezależnie od formatów stosowanych w takim warstwowym podejściu GR29 zaleca, by w pierwszej „warstwie" (innymi słowy – w ramach głównego sposobu, w który administrator po raz pierwszy wchodzi w interakcję z osobą, której dane dotyczą) przekazywano zasadniczo najważniejsze informacje (wskazane w pkt 36 powyżej), tj. szczegółowe informacje na temat celów przetwarzania, tożsamość administratora i wskazanie istniejących praw osoby, której dane dotyczą, a także informacje na temat najważniejszych skutków przetwarzania lub na temat przetwarzania, które może zaskoczyć osobę, której dane dotyczą. Na przykład, jeżeli pierwszy kontakt z osobą, której dane dotyczą, ma miejsce drogą telefoniczną, informacje te mogłyby zostać przekazane podczas rozmowy telefonicznej, a pozostałe informacje wymagane na podstawie art. 13 i 14 mogłyby zostać jej przekazane za pośrednictwem innych, dodatkowych środków, takich jak przesłanie kopii polityki ochrony prywatności w wiadomości e-mail lub przesłanie osobie, której dane dotyczą, linku do warstwowego internetowego oświadczenia o ochronie prywatności / warstwowej internetowej informacji o polityce prywatności administratora.

Powiadomienia typu „push" i „pull"

39. Innym możliwym sposobem dostarczania informacji dotyczących przejrzystości są powiadomienia typu „push" i „pull". Powiadomienia typu „push" obejmują wysyłanie powiadomień zawierających informacje dotyczące przejrzystości typu „just-in-time", natomiast powiadomienia typu „pull" ułatwiają dostęp do informacji za pomocą takich metod, jak zarządzanie pozwoleniem, pulpity nawigacyjne prywatności oraz samouczki „dowiedz się więcej". Zapewniają one osobie, której dane dotyczą, przekazanie informacji o przejrzystości w sposób bardziej ukierunkowany na użytkownika.

- Pulpit nawigacyjny prywatności jest jednym punktem, z którego osoby, których dane dotyczą, mogą przeglądać informacje na temat ochrony prywatności i zarządzać swoimi preferencjami w zakresie prywatności, zezwalając na określone sposoby wykorzystania danych, które ich dotyczą, przez daną usługę albo uniemożliwiając takie wykorzystanie. Jest to szczególnie przydatne w przypadku korzystania przez osoby, których dane dotyczą, z tej samej usługi na różnych urządzeniach, ponieważ zapewnia im dostęp do swoich danych osobowych i kontrolę nad nimi bez względu na sposób korzystania z usługi. Umożliwienie osobom, których dane dotyczą, ręcznego dostosowania ustawień prywatności za pośrednictwem pulpitu nawigacyjnego prywatności może również ułatwić spersonalizowanie oświadczenia o ochronie prywatności / informacji o polityce prywatności poprzez uwzględnienie jedynie tych rodzajów przetwarzania, które mają miejsce w przypadku danej osoby. Pożądane jest włączenie pulpitu nawigacyjnego prywatności do istniejącej architektury usługi (np. wykorzystując ten sam wzór i tę samą markę, co w przypadku pozostałej części usługi), ponieważ zapewni to intuicyjność dostępu do pulpitu oraz korzystania z niego, a także może zachęcić użytkowników do zainteresowania się informacjami o prywatności na równi z innymi aspektami usługi. Może być to skuteczny sposób wykazania, że informacje na temat ochrony prywatności stanowią konieczną i integralną część usługi, a nie długie wykazy napisane żargonem prawnym.

- Powiadomienie typu „just-in-time" jest wykorzystywane w celu przekazania konkretnych informacji dotyczących prywatności na zasadzie *ad hoc* – w najodpowiedniejszym czasie dla osoby, której dane dotyczą. Metoda ta jest przydatna do przekazywania informacji na różnych etapach procesu pozyskiwania danych; pomaga podzielić przekazywane informacje na krótsze, łatwiejsze do zrozumienia części, dzięki czemu administratorzy danych mogą w mniejszym stopniu korzystać z oświadczenia o ochronie prywatności / informacji o polityce prywatności w formie jednego ciągłego dokumentu, który jest trudny do zrozumienia bez kontekstu. Na przykład, jeżeli osoba, której dane dotyczą, zakupi produkt przez internet, krótkie informacje wyjaśniające można podać w wyskakujących okienkach towarzyszących odpowiednim polom tekstu. Informacje podane obok pola zawierającego prośbę o numer telefonu osoby, której dane dotyczą, mogłyby na przykład zawierać wyjaśnienie, że dane te są zbierane wyłącznie do celów kontaktów w sprawie zakupu oraz że zostaną ujawnione wyłącznie do celów usługi doręczenia.

Inne rodzaje „odpowiednich środków"

40. Biorąc pod uwagę bardzo wysoki poziom dostępu do internetu w UE oraz fakt, że osoby, których dane dotyczą, mogą uzyskać dostęp do internetu w dowolnym momencie, z wielu miejsc i z wielu urządzeń, GR29 jest zdania – jak już stwierdzono powyżej – że „odpowiednim środkiem" służącym przekazaniu informacji dotyczących przejrzystości w przypadku administratorów danych, którzy działają w środowisku cyfrowym/online, jest elektroniczne oświadczenie o ochronie prywatności / elektroniczna informacja o polityce prywatności. Ze względu na okoliczności pozyskiwania i przetwarzania danych administrator może jednak stwierdzić konieczność dodatkowego (lub alternatywnego – jeżeli administrator danych nie działa w środowisku cyfrowym/online) stosowania innych sposobów oraz formatów przekazywania informacji. Inne możliwe sposoby przekazywania informacji osobie, której dane dotyczą, związane z następującymi różnymi środowiskami danych osobowych, mogą obejmować następujące sposoby właściwe w określonym, wskazanym poniżej środowisku. Jak zauważono powyżej, administratorzy mogą przyjąć podejście warstwowe, gdy decydują się na zastosowanie kombinacji takich metod, zapewniając jednocześnie, by najważniejsze informacje (zob. pkt 36 i 38) zawsze były

przekazywane za pośrednictwem pierwszego sposobu wykorzystywanego do komunikacji z osobą, której dane dotyczą.

a. Forma papierowa np. w przypadku zawierania umów drogą pocztową: wyjaśnienia pisemne, ulotki, informacje w dokumentacji umownej, komiksy, infografiki lub schematy blokowe;
b. Łączność telefoniczna: wyjaśnienia ustne przez człowieka, aby umożliwić interakcję i udzielanie odpowiedzi na pytania, albo zautomatyzowane bądź nagrane wcześniej informacje umożliwiające wybór opcji odsłuchania bardziej szczegółowych informacji;
c. Technologie urządzeń inteligentnych bez ekranu / środowisko internetu rzeczy, takie jak analiza śledzenia Wi-Fi: znaki graficzne, kody QR, ostrzeżenia głosowe, informacje pisemne zawarte w papierowych instrukcjach konfiguracji, filmy wideo zawarte w cyfrowych instrukcjach konfiguracji, informacje pisemne na temat urządzenia inteligentnego, wiadomości wysłane SMS-em lub pocztą elektroniczną, widoczne tablice zawierające informacje, oznakowanie informacyjne lub publiczne kampanie informacyjne;
d. Kontakty bezpośrednie, takie jak udział w sondażu opinii publicznej, osobista rejestracja w celu skorzystania z usługi: wyjaśnienia ustne lub pisemne przekazane w formie papierowej lub elektronicznej;
e. Środowisko „rzeczywiste", w którym prowadzone są nagrania z użyciem CCTV / bezzałogowych statków powietrznych: widoczne tablice zawierające informacje, oznakowanie informacyjne, publiczne kampanie informacyjne lub ogłoszenia w gazetach / mediach.

Informacje dotyczące profilowania i zautomatyzowanego podejmowania decyzji

41. Informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i art. 22 ust. 4, wraz z istotnymi informacjami o zasadach ich podejmowania, a także o znaczących i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą, stanowią część obowiązkowych informacji, które należy przekazać tej osobie zgodnie z art. 13 ust. 2 lit. f) i art. 14 ust. 2 lit. g). GR29 sporządziła wytyczne dotyczące zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania[35], do których należy się odwołać w celu uzyskania dalszych wskazówek na temat sposobu zapewnienia przejrzystości w określonych sytuacjach związanych z profilowaniem. Należy zauważyć, że oprócz szczególnych wymogów w zakresie przejrzystości mających zastosowanie do zautomatyzowanego podejmowania decyzji na podstawie art. 13 ust. 2 lit. f) oraz art. 14 ust. 2 lit. g) zawarte w tych wytycznych uwagi dotyczące znaczenia informowania osób, których dane dotyczą, o konsekwencjach przetwarzania ich danych osobowych, a także określona w nich ogólna zasada, zgodnie z którą nie można zaskakiwać osoby przetwarzaniem jej danych, mają również zastosowanie do profilowania w ujęciu ogólnym (a nie tylko profilowania, o którym mowa w art. 22[36]), jako rodzaju przetwarzania[37].

[35] Wytyczne w sprawie zautomatyzowanego podejmowania decyzji i profilowania do celów rozporządzenia 2016/679, GR 251.

Inne kwestie – ryzyko, zasady i zabezpieczenia

42. Motyw 39 RODO odnosi się również do przekazywania określonych informacji, które nie są wyraźnie objęte zakresem stosowania art. 13 i art. 14 (zob. tekst motywu powyżej w pkt 28). Zawarte w tym motywie odniesienie do uświadamiania osobom, których dane dotyczą, ryzyka, zasad i zabezpieczeń w odniesieniu do przetwarzania danych osobowych jest związane z szeregiem innych kwestii. Obejmują one oceny skutków dla ochrony danych. Jak wskazano w wytycznych GR29 dotyczących ocen skutków dla ochrony danych[38], administratorzy danych mogą rozważyć publikację oceny skutków dla ochrony danych (lub jej części) w ramach zwiększania zaufania do operacji przetwarzania oraz wykazania przejrzystości i rozliczalności, chociaż jej publikacja nie jest obowiązkowa. Ponadto przestrzeganie kodeksu postępowania (przewidzianego w art. 40) może mieć na celu wykazanie przejrzystości, ponieważ kodeksy postępowania mogą być sporządzane w celu doprecyzowania stosowania RODO między innymi w odniesieniu do: rzetelnego i przejrzystego przetwarzania; informowania opinii publicznej i osób, których dane dotyczą; informowania i ochrony dzieci.

43. Inną istotną kwestią związaną z przejrzystością jest uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych (zgodnie z wymogami określonymi w art. 25). Zgodnie z tymi zasadami administratorzy danych muszą od samego początku uwzględniać kwestie ochrony danych w swoich operacjach i systemach przetwarzania, a nie traktować ją jako formalność do dopełnienia w ostatniej chwili. Motyw 78 odnosi się do środków wykonawczych administratorów danych, które spełniają wymogi w zakresie ochrony danych w fazie projektowania oraz domyślnej ochrony danych, w tym środków polegających na zapewnieniu przejrzystości w odniesieniu do funkcji i przetwarzania danych osobowych.

44. Niezależnie od tego, zadania współadministratorów również wiążą się z uświadamianiem osobom, których dane dotyczą, ryzyka, zasad i zabezpieczeń. Zgodnie z art. 26 ust. 1 współadministratorzy w przejrzysty sposób określają odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z RODO, w szczególności w odniesieniu do wykonywania przez osobę, której dane dotyczą, przysługujących jej praw oraz ich obowiązków w odniesieniu do podawania informacji, o których mowa w art. 13 i 14. Zgodnie z art. 26 ust. 2 zasadnicza treść uzgodnień między administratorami danych jest udostępniana osobom, których dane dotyczą. Innymi słowy,

[36] Zasada ta ma zastosowanie do procesu podejmowania decyzji polegającego wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, które wywołuje skutki prawne wobec osoby, której dane dotyczą, lub w podobny sposób istotnie na nią wpływa.
[37] Istotne znaczenie ma w tym kontekście motyw 60, który stanowi: „Ponadto należy poinformować osobę, której dane dotyczą, o fakcie profilowania oraz o konsekwencjach takiego profilowania".
[38] Wytyczne dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko" do celów rozporządzenia 2016/679, GR 248 rev.1

osoba, której dane dotyczą, musi mieć całkowitą pewność, do którego administratora danych może się zwrócić, jeżeli zamierza wykonać prawo lub prawa przysługujące jej na podstawie RODO[39].

Informacje związane z dalszym przetwarzaniem

45. Zarówno art. 13, jak i art. 14 zawierają przepis[40] nakładający na administratora danych wymóg poinformowania osoby, której dane dotyczą, jeżeli planuje on dalej przetwarzać jej dane osobowe w celu innym niż cel, w którym dane osobowe zostały zebrane/pozyskane. W takim przypadku „przed takim dalszym przetwarzaniem informuje on osobę, której dane dotyczą, o tym innym celu oraz udziela jej wszelkich innych stosownych informacji, o których mowa w ust. 2". Przepisy te wprowadzają w życie zasadę określoną w art. 5 ust. 1 lit. b), zgodnie z którą dane osobowe są zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach, przy czym dalsze przetwarzanie w sposób *niezgodny* z tymi celami jest zabronione[41]. Część druga art. 5 ust. 1 lit. b) stanowi, że dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 za niezgodne z pierwotnymi celami. W przypadku dalszego przetwarzania danych osobowych do celów *zgodnych* z pierwotnymi celami (art. 6 ust. 4 zawiera informacje dotyczące tej kwestii[42]) zastosowanie mają art. 13 ust. 3 i art. 14 ust. 4. Zawarty w powyższych artykułach wymóg informowania osób, których dane dotyczą, o dalszym przetwarzaniu propaguje określone w RODO stanowisko, zgodnie z którym w czasie i w kontekście, w którym zbierane są dane osobowe, osoba, której dane dotyczą, powinna mieć rozsądne przesłanki, by spodziewać się, że może nastąpić przetwarzanie danych w tym celu[43]. Innymi słowy, osoba, której dane dotyczą, nie powinna być zaskoczona celem przetwarzania jej danych osobowych.

46. Art. 13 ust. 3 i art. 14 ust. 4 – w zakresie, w jakim odnoszą się do udzielenia „wszelkich innych stosownych informacji, o których mowa w ust. 2" – można na pierwszy rzut oka interpretować jako pozostawiające administratorowi danych pewien stopień swobody wyboru co do zakresu i konkretnych kategorii informacji określonych w odpowiednim ust. 2 (tj., w zależności od przypadku, art. 13 ust. 2 albo art. 14 ust. 2), których należy udzielić osobie, której dane dotyczą. (W motywie 61 określono je mianem „innych niezbędnych informacji".) Zasadnicze stanowisko jest jednak takie, że osobie, której dane dotyczą, należy udzielić wszystkich tego rodzaju informacji określonych w tym ustępie, chyba że przynajmniej jedna kategoria informacji nie istnieje lub nie ma zastosowania.

47. GR29 zaleca, aby w celu zapewnienia przejrzystości, rzetelności i rozliczalności administratorzy rozważyli udostępnienie osobom, których dane dotyczą, w oświadczeniu o ochronie prywatności / informacji o polityce prywatności informacji o analizie zgodności przeprowadzanej zgodnie z art. 6 ust. 4[44], jeżeli nowy cel przetwarzania opiera się na podstawie prawnej innej niż zgoda lub prawo krajowe / unijne. (Innymi słowy, wyjaśnienie, w jaki sposób przetwarzanie w innym celu (w innych celach) jest zgodne z pierwotnym celem). Celem jest zapewnienie osobom, których dane dotyczą, możliwości rozważenia zgodności dalszego przetwarzania i udzielonych zabezpieczeń, a także podjęcia decyzji o ewentualnym wykonaniu przysługujących im praw, tj. m.in. prawa do ograniczenia przetwarzania lub prawa do wniesienia sprzeciwu wobec przetwarzania[45]. Jeżeli administratorzy postanowią nie włączać takich informacji do informacji o polityce prywatności / oświadczenia o ochronie prywatności, GR29 zaleca, by wyjaśnili osobom, których dane dotyczą, że mogą otrzymać te informacje na wniosek.

48. Z wykonywaniem przez osobę, której dane dotyczą, przysługujących jej praw wiąże się kwestia czasu. Jak podkreślono powyżej, przekazanie informacji w odpowiednim czasie jest kluczowym elementem wymogów dotyczących przejrzystości określonych w art. 13 i 14 i jest nieodłącznie związane z koncepcją rzetelnego przetwarzania. Informacje dotyczące *dalszego przetwarzania* należy przekazać „przed takim dalszym przetwarzaniem". GR29 stoi na stanowisku, że należy zapewnić rozsądny okres pomiędzy powiadomieniem a rozpoczęciem przetwarzania, a nie rozpoczynać przetwarzanie bezzwłocznie po otrzymaniu powiadomienia przez osobę, której dane dotyczą. Przynosi to osobom, których dane dotyczą, praktyczne korzyści wynikające z zasady przejrzystości, dając im faktyczną możliwość rozważenia dalszego przetwarzania (i ewentualnego wykonania związanych z tym praw). Pojęcie „rozsądny termin" zależy od danej sytuacji. Zgodnie z zasadą rzetelności im bardziej inwazyjne (lub im mniej spodziewane) jest dalsze przetwarzanie, tym okres ten powinien być dłuższy. Zgodnie z zasadą rozliczalności administratorzy danych powinni być też w stanie wykazać, w jaki sposób okoliczności uzasadniają ustalenia dokonane przez nich w odniesieniu do czasu przekazania tych informacji oraz dlaczego taki termin jest rzetelny wobec osób, których dane dotyczą. (Zob. również uwagi dotyczące ustalania rozsądnych terminów powyżej w pkt 30–32.)

Narzędzia wizualizacyjne

49. Co istotne, zasada przejrzystości określona w RODO nie ogranicza się jedynie do komunikacji językowej (pisemnej czy ustnej). W RODO przewidziano w stosownych przypadkach narzędzia wizualizacyjne (w szczególności odniesienia, znaki graficzne, mechanizmy certyfikacji oraz znaki jakości i oznaczenia w dziedzinie ochrony danych).

[39] Zgodnie z art. 26 ust. 3 niezależnie od dokonanych przez współadministratorów uzgodnień, o których mowa w art. 26 ust. 1, osoba, której dane dotyczą, może wykonywać przysługujące jej prawa wynikające z RODO wobec każdego ze współadministratorów.

[40] Art. 13 ust. 3 i art. 14 ust. 4 mają identyczne brzmienie, z wyjątkiem słowa „zebrane", którego użyto w art. 13 i który zastąpiono słowem „pozyskane" w art. 14.

[41] W odniesieniu do tej zasady zob. np. motywy 47, 50, 61, 156 i 158; art. 6 ust. 4 i art. 89.

[42] Art. 6 ust. 4 zawiera katalog otwarty czynników, które należy uwzględnić, aby ustalić, czy przetwarzanie w innym celu jest zgodne z celem, w którym dane osobowe zostały pierwotnie zebrane, tj.: związek między celami, kontekst, w którym zebrano dane osobowe; charakter danych osobowych (w szczególności czy przetwarzane są szczególne kategorie danych osobowych lub dane osobowe dotyczące naruszeń prawa i wyroków skazujących); ewentualne konsekwencje zamierzonego dalszego przetwarzania dla osób, których dane dotyczą; istnienie odpowiednich zabezpieczeń.

[43] Motywy 47 i 50.

[44] Mowa o tym również w motywie 50.

[45] Jak wskazano w motywie 63, umożliwi to osobie, której dane dotyczą, wykonywanie prawa dostępu, by mieć świadomość przetwarzania i móc zweryfikować zgodność przetwarzania z prawem.

W motywie 58[46] wskazano, że dostępność informacji kierowanych do ogółu społeczeństwa lub osób, których dane dotyczą, ma szczególne znaczenie w środowisku online[47].

Znaki graficzne

50. W motywie 60 przewidziano przekazywanie informacji osobie, której dane dotyczą, „w połączeniu" ze standardowymi znakami graficznymi, umożliwiając tym samym warstwowe podejście. Wykorzystywanie znaków graficznych nie powinno jednak po prostu zastępować informacji koniecznych do wykonywania przez osobę, której dane dotyczą, przysługujących jej praw ani nie należy traktować tego rodzaju znaków jako elementu zastępującego konieczność wykonywania przez administratora danych obowiązków nałożonych na niego na podstawie art. 13 i 14. W art. 12 ust. 7 przewidziano wykorzystywanie takich znaków graficznych, stwierdzając, że:

> „Informacje, których udziela się osobom, których dane dotyczą, na mocy art. 13 i 14, można opatrzyć standardowymi znakami graficznymi, które w widoczny, zrozumiały i czytelny sposób przedstawią sens zamierzonego przetwarzania. Jeżeli znaki te są przedstawione elektronicznie, muszą się nadawać do odczytu maszynowego".

51. Ponieważ art. 12 ust. 7 stanowi, że „jeżeli znaki te są przedstawione elektronicznie, muszą się nadawać do odczytu maszynowego", sugeruje to, iż mogą wystąpić sytuacje, w których znaki graficzne nie są przedstawiane elektronicznie[48], na przykład znaki graficzne na dokumentach w formie papierowej, urządzeniach połączonych za pośrednictwem internetu lub opakowaniach takich urządzeń, powiadomieniach w miejscach publicznych dotyczących śledzenia Wi-Fi, kodach QR oraz powiadomieniach dotyczących CCTV.

[46] „Informacje te mogą być przekazywane w formie elektronicznej, na przykład za pomocą strony internetowej, gdy są kierowane do ogółu społeczeństwa. Dotyczy to w szczególności sytuacji, gdy duża liczba podmiotów i złożoność technologiczna działań sprawiają, że osobie, której dane dotyczą, trudno jest dowiedzieć się i zrozumieć, czy dotyczące jej dane osobowe są zbierane, przez kogo oraz w jakim celu, na przykład w przypadku reklamy w internecie".

[47] W tym kontekście administratorzy powinni uwzględniać słabowidzące osoby, których dane dotyczą (np. cierpiące na daltonizm).

[48] RODO nie zawiera definicji pojęcia „nadający się do odczytu maszynowego", jednak w motywie 21 dyrektywy 2013/37/UE17 zdefiniowano pojęcie „przeznaczony do odczytu komputerowego" jako:
„format pliku zorganizowany w sposób umożliwiający aplikacjom komputerowym łatwe identyfikowanie, rozpoznawanie i pozyskiwanie z niego określonych danych. Dane zakodowane w plikach zorganizowanych w formacie przeznaczonym do odczytu komputerowego to dane przeznaczone do odczytu komputerowego. Formaty przeznaczone do odczytu komputerowego mogą być otwarte lub zastrzeżone; mogą one występować jako standardy formalne lub nie. Dokumentów zakodowanych w formacie pliku ograniczającym przetwarzanie automatyczne z powodu niemożności pozyskania danych lub utrudnień w ich pozyskaniu z tych dokumentów nie należy uznawać za sporządzone w formacie przeznaczonym do odczytu komputerowego. Państwa członkowskie powinny w stosownych przypadkach zachęcać do korzystania z formatów otwartych przeznaczonych do odczytu komputerowego".

52. Celem stosowania znaków graficznych jest najwyraźniej zwiększenie przejrzystości dla osób, których dane dotyczą, dzięki potencjalnemu ograniczeniu potrzeby przekazywania osobie, której dane dotyczą, ogromnych ilości informacji pisemnych. Użyteczność znaków graficznych w celu skutecznego przekazywania osobom, których dane dotyczą, informacji wymaganych zgodnie z art. 13 i 14 zależy jednak od standaryzacji symboli/rysunków, które mają być powszechnie wykorzystywane i uznawane w całej UE jako skrótowe przedstawienie tych informacji. W tym względzie w RODO nałożono odpowiedzialność za sporządzenie kodu znaków graficznych na Komisję, ale ostatecznie opinię na temat takich znaków graficznych może przedstawić Komisji, na wniosek Komisji albo z urzędu, Europejska Rada Ochrony Danych[49].GR29 przyznaje, że zgodnie z motywem 166 opracowanie kodu znaków graficznych powinno się opierać na podejściu opartym na dowodach, a zanim nastąpi jakakolwiek standaryzacja konieczne będzie przeprowadzenie, we współpracy z sektorem i ogółem społeczeństwa, szeroko zakrojonych badań dotyczących skuteczności znaków graficznych w tym kontekście.

Mechanizmy certyfikacji, znaki jakości i oznaczenia

53. Oprócz wykorzystywania standardowych znaków graficznych RODO (art. 42) odnosi się również do wykorzystywania mechanizmów certyfikacji oraz znaków jakości i oznaczeń w zakresie ochrony danych osobowych mających świadczyć o tym, że operacje przetwarzania prowadzone przez administratorów danych i podmioty przetwarzające są zgodne z RODO oraz mają na celu zwiększenie przejrzystości dla osób, których dane dotyczą[50]. GR29 wyda wytyczne dotyczące mechanizmów certyfikacji w stosownym czasie.

Wykonywanie uprawnień przysługujących osobom, których dane dotyczą

54. W świetle RODO wymóg przejrzystości oznacza dla administratorów danych potrójny obowiązek, jeżeli chodzi o prawa osób, których dane dotyczą, ponieważ są oni zobowiązani do[51]:

- udzielania osobom, których dane dotyczą, informacji dotyczących przysługujących im praw[52] (zgodnie z art. 13 ust. 2 lit. b) oraz art. 14 ust. 2 lit. c));

[49] Art. 12 ust. 8 stanowi, że Komisji przysługuje prawo przyjmowania aktów delegowanych zgodnie z art. 92 w celu określenia informacji przedstawianych za pomocą znaków graficznych i informacji dotyczących ustanowienia standardowych znaków graficznych. W motywie 166 (dotyczącym aktów delegowanych Komisji w ujęciu ogólnym), który ma charakter pouczenia, stwierdzono, że w czasie prac przygotowawczych Komisja musi prowadzić stosowne konsultacje, w tym na szczeblu eksperckim. Jednak Europejska Rada Ochrony Danych ma również do odegrania istotną rolę konsultacyjną w odniesieniu do standaryzacji znaków graficznych, ponieważ art. 70 ust. 1 lit. r) stanowi, że Europejska Rada Ochrony Danych – z urzędu lub w stosownych przypadkach na wniosek Komisji – udziela Komisji opinii w sprawie znaków graficznych.

[50] Zob. odniesienie w motywie 100.

[51] Na podstawie sekcji RODO dotyczącej przejrzystości i trybu korzystania z praw przez osobę, której dane dotyczą (rozdział III sekcja 1 art. 12)

- przestrzegania zasady przejrzystości (tj. odnoszącej się do jakości komunikacji przewidzianej w art. 12 ust. 1) podczas komunikowania się z osobami, których dane dotyczą, w zakresie ich praw określonych w art. 15–22 i art. 34; oraz
- ułatwiania osobom, których dane dotyczą, wykonywania praw przysługujących im na mocy art. 15–22.

55. Określone w RODO wymogi dotyczące wykonywania tych praw oraz charakter wymaganych informacji mają na celu zapewnienie osobom, których dane dotyczą, *realnej możliwości* dochodzenia swoich praw i pociągnięcia administratorów danych do odpowiedzialności za przetwarzanie ich danych osobowych. W motywie 59 podkreślono, że „należy przewidzieć procedury ułatwiające osobie, której dane dotyczą, wykonywanie praw" oraz że administrator danych powinien „zapewnić możliwość wnoszenia odnośnych żądań także drogą elektroniczną, w szczególności gdy dane osobowe są przetwarzane drogą elektroniczną". Sposób, w jaki administrator danych zapewnia osobom, których dane dotyczą, możliwość wykonania przysługujących im praw, powinien być odpowiedni do kontekstu i charakteru stosunków oraz interakcji między administratorem a osobą, której dane dotyczą. W tym celu administrator danych może zdecydować się zapewnić inną metodę wykonania praw lub większą liczbę takich innych metod, aby uwzględnić szczególne sposoby interakcji osób, których dane dotyczą, z administratorami danych.

Przykład

Podmiot świadczący usługi zdrowotne udostępnia formularz elektroniczny na swojej stronie internetowej oraz formularze w formie papierowej w recepcjach przychodni, aby ułatwić składanie wniosków o udostępnienie danych osobowych zarówno online, jak i osobiście. Obok tych metod placówka zdrowotna przyjmuje wnioski o udostępnienie danych składane inną drogą (na przykład listownie lub e-mailem) oraz zapewnia dedykowany punkt kontaktowy (do którego można uzyskać dostęp drogą e-mailową lub telefonicznie), aby pomóc osobom, których dane dotyczą, w wykonywaniu przysługujących im praw.

Wyjątki od obowiązku udzielenia informacji

Wyjątki określone w art. 13

56. Jedyny wyjątek od ciążących na administratorze danych obowiązków określonych w art. 13 – jeżeli zebrał on dane osobowe bezpośrednio od osoby, której dane dotyczą – występuje, „gdy – i w zakresie, w jakim – osoba, której dane dotyczą, dysponuje już tymi informacjami"[53]. Zgodnie z zasadą rozliczalności administratorzy danych muszą wykazać (i udokumentować), jakie informacje posiada już osoba, której dane dotyczą, w jaki sposób i kiedy je otrzymała oraz że od tego czasu nie nastąpiły żadne zmiany w tych informacjach, które spowodowałyby ich dezaktualizację. Ponadto zastosowanie w art. 13 ust. 4 wyrażenia „w zakresie, w jakim" wyjaśnia, że nawet jeżeli osobie, której dane dotyczą, przekazano już pewne kategorie informacji z wykazu informacji zawartego w art. 13, na administratorze danych wciąż spoczywa obowiązek uzupełnienia tych informacji w celu zapewnienia, by osoba, której dane dotyczą, posiadała kompletny zestaw informacji wymienionych w art. 13 ust. 1 i art. 13 ust. 2. Następujący przykład to najlepsza praktyka dotycząca preferowanej wykładni zawężającej wyjątku określonego w art. 13 ust. 4.

[51] Praw dostępu do danych, ich sprostowania lub usunięcia, ograniczenia przetwarzania, sprzeciwu wobec przetwarzania, przenoszenia danych.
[53] Art. 13 ust. 4.

Przykład

Osoba fizyczna rejestruje się w celu korzystania z internetowej usługi poczty elektronicznej, otrzymując wszystkie informacje wymagane zgodnie z art. 13 ust. 1 i art. 13 ust. 2 w chwili rejestracji. Sześć miesięcy później osoba, której dane dotyczą, aktywuje połączoną funkcję wiadomości błyskawicznej za pośrednictwem dostawcy usług poczty elektronicznej i podaje w tym celu swój numer telefonu komórkowego. Usługodawca przekazuje osobie, której dane dotyczą, niektóre informacje określone w art. 13 ust. 1 i art. 13 ust. 2 dotyczące przetwarzania numeru telefonu (np. dotyczące celów i podstawy prawnej przetwarzania, odbiorców, okresu zatrzymywania), ale nie przekazuje innych informacji, które osoba ta posiada już od 6 miesięcy i które się nie zmieniły (np. tożsamości i danych kontaktowych administratora oraz inspektora ochrony danych, informacji dotyczących praw osoby, której dane dotyczą, oraz prawa do wniesienia skargi do właściwego organu nadzorczego). Zgodnie z najlepszą praktyką osoba, której dane dotyczą, powinna jednak ponownie otrzymać pełen zestaw informacji, ale powinna być również w stanie z łatwością stwierdzić, które z podanych informacji są nowe. Nowe przetwarzanie do celów usługi wiadomości błyskawicznej może wpłynąć na osobę, której dane dotyczą, w sposób skłaniający ją do wykonania przysługującego jej prawa, o którym mogła zapomnieć z uwagi na fakt, że poinformowano ją o nim sześć miesięcy wcześniej. Ponowne udzielenie wszystkich informacji pozwala zapewnić, by osoba, której dane dotyczą, w dalszym ciągu była dobrze poinformowana, w jaki sposób wykorzystywane są jej dane i jak może korzystać ze swoich praw.

Wyjątki określone w art. 14

57. W art. 14 ustanowiono znacznie szerszy katalog wyjątków od ciążącego na administratorze danych obowiązku udzielenia informacji, jeżeli danych osobowych nie pozyskano od osoby, której dane dotyczą. Co do zasady należy dokonywać wykładni tych wyjątków oraz stosować je w sposób zawężający. Oprócz sytuacji, w której osoba, której dane dotyczą, posiada już przedmiotowe informacje (art. 14 ust. 5 lit. a)), w art. 14 ust. 5 dopuszczono również następujące wyjątki:

- udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku; w szczególności w przypadku przetwarzania do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych lub o ile obowiązek ten mógłby uniemożliwić lub poważnie utrudnić realizację celów takiego przetwarzania;
- administrator danych podlega określonemu w prawie krajowym lub prawie Unii wymogowi pozyskania lub ujawnienia danych osobowych, przy czym w prawie tym przewidziano odpowiednią ochronę uzasadnionych interesów osoby, której dane dotyczą; lub
- dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie Unii lub w prawie państwa członkowskiego, w tym ustawowym obowiązkiem zachowania tajemnicy.

Okazuje się niemożliwe, niewspółmiernie duży wysiłek oraz poważne utrudnienie realizacji celów

58. W art. 14 ust. 5 lit. b) przewidziano 3 odrębne sytuacje, w których uchylony zostaje obowiązek udzielenia informacji określony w art. 14 ust. 1, art. 14 ust. 2 i art. 14 ust. 4:

(i) jeżeli okazuje się to niemożliwe (w szczególności do celów archiwalnych, do celów badań naukowych/historycznych lub do celów statystycznych);
(ii) jeżeli wymagałoby niewspółmiernie dużego wysiłku (w szczególności do celów archiwalnych, do celów badań naukowych/historycznych lub do celów statystycznych); lub
(iii) jeżeli udzielenie informacji wymaganych zgodnie z art. 14 ust. 1 mogłoby uniemożliwić lub poważnie utrudnić realizację celów takiego przetwarzania.

„Okazuje się niemożliwe"

59. Sytuacja, w której zgodnie z art. 14 ust. 5 lit. b) udzielenie informacji „okazuje się niemożliwe", jest sytuacją zero-jedynkową, ponieważ dana sytuacja albo jest niemożliwa, albo jest możliwa; nie istnieją stopnie „niemożliwości". Jeżeli administrator danych zamierza powołać się na to odstępstwo, musi wskazać czynniki, które faktycznie *uniemożliwiają mu* udzielenie odnośnych informacji osobom, których dane dotyczą. Jeżeli po upływie określonego czasu czynniki, które spowodowały „niemożliwość", przestaną istnieć i administrator danych uzyska możliwość udzielenia informacji osobom, których dane dotyczą, powinien bezzwłocznie to uczynić. W praktyce istnieje bardzo niewiele sytuacji, w których administrator danych może wykazać faktyczną niemożliwość udzielenia informacji osobom, których dane dotyczą. Kwestię tę ilustruje następujący przykład.

Przykład

Osoba, której dane dotyczą, rejestruje się w celu korzystania z usługi subskrypcji online na zasadzie abonamentowej. Po rejestracji administrator danych zbiera od biura informacji kredytowej dane dotyczące wiarygodności kredytowej osoby, której dane

dotyczą, aby podjąć decyzję, czy ma świadczyć usługę. Protokół administratora danych ma na celu poinformowanie osób, których dane dotyczą, o zebraniu danych dotyczących wiarygodności kredytowej w terminie trzech dni od dnia ich zebrania – zgodnie z art. 14 ust. 3 lit. a). Adres i numer telefonu osoby, której dane dotyczą, nie figurują jednak w rejestrach publicznych (osoba, której dane dotyczą, mieszka za granicą). Podczas rejestracji w celu korzystania z usługi osoba, której dane dotyczą, nie podała swojego adresu e-mail lub adres ten jest nieprawidłowy. Administrator stwierdza, że nie ma możliwości bezpośredniego skontaktowania się z osobą, której dane dotyczą. W tym przypadku administrator może jednak udzielić informacji o zbieraniu danych dotyczących kredytów na swojej stronie internetowej przed rejestracją. W tym przypadku udzielenie informacji zgodnie z art. 14 nie byłoby niemożliwe.

Niemożność podania źródła danych

60. W motywie 61 stwierdzono, że „jeżeli osobie, której dane dotyczą, nie można podać pochodzenia danych osobowych, ponieważ korzystano z różnych źródeł, informacje należy przedstawić w sposób ogólny". Uchylenie wymogu udzielenia osobom, których dane dotyczą, informacji dotyczących źródła ich danych osobowych ma zastosowanie wyłącznie wówczas, gdy nie jest to możliwe, ponieważ nie można przypisać różnych danych osobowych dotyczących tej samej osoby, której dane dotyczą, do konkretnego źródła. Przykładowo sam fakt, że baza danych obejmująca dane osobowe wielu osób została skompilowana przez administratora z wykorzystaniem więcej niż jednego źródła, nie wystarcza, by uchylić ten wymóg, jeżeli można (chociaż jest to czasochłonne lub uciążliwe) określić źródło, z którego pochodzą dane osobowe poszczególnych osób. Biorąc pod uwagę wymogi dotyczące uwzględniania ochrony danych w fazie projektowania oraz domyślnej ochrony danych[54], systemy przetwarzania powinny być od początku wyposażone w mechanizmy przejrzystości, tak by wszystkie źródła danych osobowych otrzymywanych przez organizację można było monitorować, a także prześledzić ich historię aż do źródła na każdym etapie przetwarzania danych (zob. pkt 43 powyżej).

„Niewspółmiernie duży wysiłek"

61. Zgodnie z art. 14 ust. 5 lit. b), podobnie jak w sytuacji, w której przetwarzanie „okazuje się niemożliwe", może również mieć zastosowanie „niewspółmiernie duży wysiłek", zwłaszcza w przypadku przetwarzania „do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, z zastrzeżeniem warunków i zabezpieczeń, o których mowa w art. 89 ust. 1". W motywie 62 odniesiono się również do tych celów jako do przypadków, w których udzielenie informacji osobie, której dane dotyczą, wymagałoby niewspółmiernie dużego wysiłku, przy czym stwierdzono w nim, że uwzględnić przy tym należy liczbę osób, których dane dotyczą, okres przechowywania

[54] Art. 25

danych oraz wszelkie przyjęte odpowiednie zabezpieczenia. Biorąc pod uwagę nacisk, jaki położono w motywie 62 i w art. 14 ust. 5 lit. b) na cele archiwalne, cele badań naukowych i cele statystyczne w odniesieniu do stosowania tego odstępstwa, GR29 stoi na stanowisku, że wyjątek ten nie powinien być *rutynowo* stosowany przez administratorów danych, którzy nie przetwarzają danych osobowych do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych. GR29 podkreśla, że w przypadkach gdy są to zamierzone cele, należy wciąż spełnić warunki określone w art. 89 ust. 1 i udzielenie informacji musi wiązać się z niewspółmiernie dużym wysiłkiem.

62. Przy określaniu, co może stanowić niemożliwość albo niewspółmiernie duży wysiłek zgodnie z art. 14 ust. 5 lit. b), istotne jest, że nie istnieją porównywalne wyłączenia na podstawie art. 13 (gdy dane osobowe są zbierane od osoby, której dane dotyczą). Jedyną różnicą między sytuacją określoną w art. 13 a sytuacją określoną w art. 14 jest fakt, że w tym ostatnim przypadku dane osobowe nie są zbierane od osoby, której dane dotyczą. Wynika z tego zatem, że niemożliwość lub niewspółmiernie duży wysiłek wynikają co do zasady z okoliczności, które nie występują, jeżeli dane osobowe są zbierane od osoby, której dane dotyczą. Innymi słowy, niemożliwość lub niewspółmiernie duży wysiłek muszą bezpośrednio wynikać z faktu, że dane osobowe zebrano w inny sposób niż od osoby, której dane dotyczą.

Przykład

Duży szpital metropolitalny wymaga od wszystkich pacjentów z oddziału dziennego, przyjętych na dłuższy okres i zgłaszających się na wizytę wypełnienia formularza informacji o pacjencie, w którym należy podać dane dwóch osób bliskich (osób, których dane dotyczą). Biorąc pod uwagę bardzo dużą liczbę pacjentów korzystających codziennie z usług szpitala, niewspółmiernie dużego wysiłku ze strony szpitala wymagałoby udzielenie wszystkim osobom, które zostały wymienione jako „osoby bliskie" na formularzach wypełnianych każdego dnia przez pacjentów, informacji wymaganych zgodnie z art. 14.

63. Czynniki, o których mowa powyżej w motywie 62 (liczba osób, których dane dotyczą, okres przechowywania danych oraz wszelkie przyjęte odpowiednie zabezpieczenia), mogą wskazywać na rodzaje kwestii, które przyczyniają się do konieczności podjęcia przez administratora danych niewspółmiernie dużego wysiłku w celu udzielenia osobie, której dane dotyczą, istotnych informacji zgodnie z art. 14.

Przykład

Naukowcy zajmujący się badaniami historycznymi, którzy chcą prześledzić pochodzenie na podstawie nazwisk, pośrednio uzyskują obszerny zbiór danych dotyczących 20 000 osób. Dane należące do zbioru zostały jednak zebrane 50 lat temu i nie były od tego czasu aktualizowane oraz nie zawierają żadnych danych kontaktowych. Biorąc pod uwagę wielkość bazy danych, a w szczególności okres

przechowywania danych, podjęcie przez naukowców indywidualne próby odnalezienia osób, których dane dotyczą, w celu udzielenia im informacji określonych w art. 14 wymagałoby niewspółmiernie dużego wysiłku.

64. Jeżeli administrator danych ma zamiar powołać się na wyjątek określony w art. 14 ust. 5 lit. b) na tej podstawie, że udzielenie informacji wymagałoby niewspółmiernie dużego wysiłku, powinien przeprowadzić test równowagi, aby porównać wysiłek wkładany przez administratora danych w udzielenie informacji osobie, której dane dotyczą, z konsekwencjami i skutkami dla tej osoby w przypadku nieudzielenia tego rodzaju informacji. Administrator danych powinien udokumentować tę ocenę zgodnie ze spoczywającymi na nim obowiązkami w zakresie rozliczalności. W takim przypadku art. 14 ust. 5 lit. b) stanowi, że administrator musi wprowadzić odpowiednie środki, by chronić prawa i wolności oraz prawnie uzasadnione interesy osoby, której dane dotyczą. Zasada ta ma zastosowanie również wówczas, gdy administrator uzna, że udzielenie informacji jest niemożliwe lub mogłoby uniemożliwić lub poważnie utrudnić realizację celów przetwarzania. Jednym z odpowiednich środków – zgodnie z art. 14 ust. 5 lit. b) – jakie administrator musi zawsze podejmować, jest udostępnianie informacji publicznie. Administrator może udostępnić informacje publicznie na wiele sposobów, na przykład umieszczając informacje na swojej stronie internetowej lub aktywnie je ogłaszając w gazecie bądź na plakatach w swojej siedzibie. Inne odpowiednie środki – oprócz udostępniania informacji publicznie – będą zależały od okoliczności przetwarzania, lecz mogą obejmować: przeprowadzenie oceny skutków dla ochrony danych; zastosowanie technik pseudonimizacji danych; zminimalizowanie ilości zbieranych danych i okresu ich przechowywania; oraz wdrażanie środków technicznych i organizacyjnych w celu zapewnienia wysokiego poziomu bezpieczeństwa. Ponadto mogą zaistnieć sytuacje, w których administrator danych przetwarza dane osobowe, co nie wymaga identyfikacji osoby, której dane dotyczą (na przykład w przypadku danych pseudonimicznych). W takich przypadkach istotny może być również art. 11 ust. 1, ponieważ stanowi on, że administrator danych nie ma obowiązku zachowania, uzyskania ani przetworzenia dodatkowych informacji w celu zidentyfikowania osoby, której dane dotyczą, wyłącznie po to, by zastosować się do RODO.

Poważne utrudnienie realizacji celów

65. Ostatnią sytuacją opisaną w art. 14 ust. 5 lit. b) jest sytuacja, w której udzielenie informacji osobie, której dane dotyczą, przez administratora danych zgodnie z art. 14 ust. 1 może uniemożliwić lub poważnie utrudnić realizację celów przetwarzania. Aby powołać się na ten wyjątek, administratorzy danych muszą wykazać, że samo udzielenie informacji określonych w art. 14 ust. 1 zniweczyłoby cele przetwarzania. W szczególności powołanie się na ten aspekt art. 14 ust. 5 lit. b) zakłada, że przetwarzanie danych jest zgodne ze wszystkimi zasadami określonymi w art. 5 oraz – co najważniejsze – że w każdych okolicznościach przetwarzanie danych osobowych jest rzetelne i ma podstawę prawną.

Przykład

Bank A podlega określonemu w przepisach dotyczących przeciwdziałaniu praniu pieniędzy obowiązkowemu wymogowi zgłaszania do właściwego organu ścigania przestępstw finansowych podejrzanej działalności związanej z rachunkami prowadzonymi przez ten bank. Bank A otrzymuje od banku B (mającego siedzibę w innym państwie członkowskim) informację, że posiadacz rachunku zlecił mu dokonanie przelewu środków pieniężnych na inne konto prowadzone przez bank A, co wydaje się podejrzane. Bank A przekazuje te dane dotyczące posiadacza rachunku i podejrzanych działań właściwemu organowi ścigania przestępstw finansowych. Przedmiotowe przepisy dotyczące przeciwdziałaniu praniu pieniędzy stanowią, że przestępstwem jest ostrzeżenie posiadacza rachunku przez zgłaszający bank, że może on zostać objęty dochodzeniem regulacyjnym. W tej sytuacji zastosowanie ma art. 14 ust. 5 lit. b), ponieważ udzielenie osobie, której dane dotyczą (posiadaczowi rachunku w banku A) informacji określonych w art. 14 dotyczących przetwarzania danych osobowych posiadacza rachunku otrzymanych od banku B poważnie utrudniłoby realizację celów przepisów, w tym zapobiegania ostrzeżeniom. Wszystkim posiadaczom rachunku w banku A należy jednak przedstawić w momencie otwierania rachunku ogólne informacje, że ich dane osobowe mogą być przetwarzane do celów przeciwdziałania praniu pieniędzy.

Pozyskiwanie lub ujawnianie jest wyraźnie uregulowane w prawie

66. Art. 14 ust. 5 lit. c) umożliwia zniesienie wymogów udzielenia informacji określonych w art. 14 ust. 1, art. 14 ust. 2 i art. 14. ust. 4, o ile pozyskiwanie lub ujawnianie danych osobowych „jest wyraźnie uregulowane prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator". Odstępstwo to jest zależne od odnośnego prawa przewidującego „odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą". Prawo takie musi bezpośrednio odnosić się do administratora danych, a przedmiotowe pozyskiwanie lub ujawnianie powinno być obowiązkowe dla administratora danych. W związku z tym administrator danych musi być w stanie wykazać, w jaki sposób przedmiotowe prawo odnosi się do niego i wymaga, aby pozyskał albo ujawnił odnośne dane osobowe. Chociaż to w prawie Unii lub państwa członkowskiego ma zostać sformułowane prawo w taki sposób, aby przewidywało „odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą", administrator danych powinien zapewnić (i być w stanie wykazać) zgodność pozyskania lub ujawnienia danych osobowych z tymi środkami. Ponadto administrator danych powinien wyraźnie poinformować osobę, której dane dotyczą, że pozyskuje lub ujawnia dane osobowe zgodnie z odnośnym prawem, o ile nie istnieje prawny zakaz uniemożliwiający administratorowi danych wykonanie tych czynności. Jest to zgodne z motywem 41 RODO, w którym stwierdzono, że taka podstawa prawna lub taki akt prawny powinny być jasne i precyzyjne, a ich zastosowanie przewidywalne dla osób im podlegających – jak wymaga tego orzecznictwo Trybunału Sprawiedliwości UE i Europejskiego Trybunału Praw Człowieka. Art. 14 ust. 5 lit. c) jednak nie będzie miał zastosowania, w przypadku gdy administrator danych podlega obowiązkowi pozyskania danych *bezpośrednio od osoby, której dane dotyczą*, w którym to przypadku zastosowanie będzie miał art. 13. W takim przypadku jedynym odstępstwem na podstawie

RODO zwalniającym administratora z obowiązku udzielenia osobie, której dane dotyczą, informacji na temat przetwarzania, będzie odstępstwo na podstawie art. 13 ust. 4 (tzn. gdy – i w zakresie, w jakim – osoba, której dane dotyczą, dysponuje już tymi informacjami). Zgodnie z art. 23 państwa członkowskie mogą jednak ustanowić na poziomie krajowym również akty prawne dotyczące dalszych szczególnych ograniczeń prawa do przejrzystości na mocy art. 12 i informacji na podstawie art. 13 i 14, o czym mowa poniżej w pkt 68.

Przykład

Na podstawie prawa krajowego organ podatkowy podlega obowiązkowemu wymogowi pozyskania od pracodawcy szczegółowych informacji na temat wynagrodzenia pracowników. Dane osobowe nie zostają pozyskane od osoby, której dane dotyczą, i w związku z tym organ podatkowy podlega wymogom określonym w art. 14. Ponieważ pozyskiwanie danych osobowych od pracodawcy przez organ podatkowy jest wyraźnie uregulowane prawem, w tym przypadku wymogi udzielenia informacji określone w art. 14 nie mają zastosowania do organu podatkowego.

Poufność wynikająca z obowiązku zachowania tajemnicy

67. Art. 14 ust. 5 lit. d) przewiduje odstępstwo od wymogu udzielenia informacji, któremu podlega administrator danych, w przypadku gdy dane osobowe „muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie Unii lub w prawie państwa członkowskiego, w tym ustawowym obowiązkiem zachowania tajemnicy". W przypadku gdy administrator danych zamierza powołać się na to odstępstwo, musi być w stanie wykazać, że właściwie je zidentyfikował i przedstawić, w jaki sposób zawodowy obowiązek zachowania tajemnicy bezpośrednio odnosi się do administratora danych, tak że nie wolno mu przekazać osobie, której dane dotyczą, wszystkich informacji określonych w art. 14 ust. 1, art. 14 ust. 2 i art. 14 ust. 4.

Przykład

Przedstawiciel zawodu medycznego (administrator danych) podlega zawodowemu obowiązkowi zachowania tajemnicy w odniesieniu do informacji medycznych dotyczących jego pacjenta. Pacjentka (w odniesieniu do której zawodowy obowiązek zachowania tajemnicy ma zastosowanie) dostarcza przedstawicielowi zawodu medycznego informacje dotyczące jej zdrowia związane z chorobą genetyczną, na którą cierpi również wielu jej krewnych. Pacjentka dostarcza również przedstawicielowi zawodu medycznego niektóre dane osobowe dotyczącego jej krewnych (osób, których dane dotyczą), którzy cierpią na tę samą chorobę. Przedstawiciel zawodu medycznego nie ma obowiązku udzielania krewnym informacji, o których mowa w art. 14, ponieważ zastosowanie ma odstępstwo określone w art. 14 ust. 5 lit. d). Jeśli przedstawiciel zawodu medycznego udzieliłby krewnym informacji, o których mowa w art. 14, naruszony zostałby obowiązek zachowania tajemnicy zawodowej, który przedstawiciel zawodu medycznego ma wobec swojego pacjenta.

Ograniczenia praw osoby, której dane dotyczą

68. Art. 23 przewiduje, że państwa członkowskie (lub UE) mogą ustanowić akty prawne dotyczące dalszych ograniczeń zakresu praw osoby, której dane dotyczą, w odniesieniu do przejrzystości i praw podmiotowych osoby, której dane dotyczą[55], jeżeli takie akty prawne nie naruszają istoty podstawowych praw i wolności oraz stanowią niezbędny i proporcjonalny środek dla zabezpieczenia jednego lub większej liczby spośród dziesięciu celów określonych w art. 23 ust. 1 lit. a)–j). W przypadku gdy krajowe akty prawne ograniczają szczególne prawa osoby, której dane dotyczą, lub ogólne obowiązki zapewnienia przejrzystości, które w przeciwnym wypadku miałyby zastosowanie do administratora danych zgodnie z RODO, administrator danych powinien być w stanie wykazać, w jaki sposób przepis krajowy ma do niego zastosowanie. Jak określono w art. 23 ust. 2 lit. h), akt prawny musi zawierać przepis o prawie osób, których dane dotyczą, do uzyskania informacji o ograniczeniach ich praw, o ile poinformowanie ich o tym nie narusza celu ograniczenia. Spójnie z powyższym oraz zgodnie z zasadą rzetelności, administrator danych powinien również poinformować osoby, których dane dotyczą, że opierają się (lub będą się opierać w przypadku wykonywania określonego prawa osoby, której dane dotyczą) na takim *krajowym ograniczeniu prawnym* dotyczącym wykonywania prawa osoby, której dane dotyczą, lub obowiązku zapewnienia przejrzystości, o ile nie narusza to celu ograniczenia prawnego. Przejrzystość jako taka wymaga od administratora danych, aby z góry przedstawił osobie, której dane dotyczą, informacje na temat jej praw oraz ewentualnych zastrzeżeń dotyczących tych praw, na które to zastrzeżenia administrator może mieć zamiar się powoływać, tak aby osoba, której dane dotyczą, nie była zaskoczona rzekomym ograniczeniem określonego prawa, gdy w późniejszym terminie będzie próbowała wykonać je w stosunku do administratora. W odniesieniu do pseudonimizacji i minimalizacji danych, oraz w zakresie, w jakim administrator danych może powoływać się na art. 11 RODO, GR29 potwierdził już wcześniej w opinii nr 3/2017[56], że art. 11 RODO należy interpretować jako sposób egzekwowania rzeczywistej minimalizacji danych pozostający bez uszczerbku dla wykonywania przez osoby, których dane dotyczą, przysługujących im praw, oraz że należy umożliwić wykonywanie praw osoby, której dane dotyczą, przy pomocy dodatkowych informacji dostarczonych przez tę osobę.

69. Ponadto w art. 85 nakłada się na państwa członkowskie wymóg, aby przyjęły przepisy pozwalające pogodzić ochronę danych osobowych z prawem do wolności wypowiedzi i informacji. Wymaga to od państw członkowskich między innymi, aby przewidziały właściwe odstępstwa lub wyjątki od niektórych przepisów RODO (w tym wymogów przejrzystości na podstawie art. 12–14) dla przetwarzania do celów wypowiedzi dziennikarskiej, akademickiej, artystycznej lub literackiej, jeśli są one niezbędne, aby pogodzić oba prawa.

[55] Jak określono w art. 12–22 oraz art. 34 i art. 5, o ile jego przepisy odpowiadają prawom i obowiązkom przewidzianym w art. 12–22.

[56] Opinia nr 03/2017 dotycząca przetwarzania danych osobowych w ramach współpracujących inteligentnych systemów transportowych (C-ITS) – zob. pkt 4.2.

Przejrzystość oraz naruszenie ochrony danych

70. GR29 opracowała oddzielne wytyczne w sprawie naruszenia ochrony danych[57], jednak do celów niniejszych wytycznych obowiązki administratora danych w odniesieniu do zawiadomienia osoby, której dane dotyczą, o naruszeniu ochrony danych muszą w pełni uwzględniać wymogi przejrzystości określone w art. 12[58]. Zawiadomienie o naruszeniu ochrony danych musi spełniać te same wymogi, opisane szczegółowo powyżej (w szczególności dotyczące jasnego i prostego języka), które mają zastosowanie do wszelkiej innej komunikacji z osobą, której dane dotyczą, w odniesieniu do jej praw lub w związku z udzielaniem informacji na podstawie art. 13 i 14.

[57] Wytyczne w sprawie powiadomień o naruszeniu ochrony danych osobowych na mocy rozporządzenia 2016/679, GR 250.

[58] Jest to wyraźnie określone w art. 12 ust. 1, w którym mowa w szczególności o „wszelkiej komunikacji z osobą, której dane dotyczą, na mocy art. 15–22 i 34 w sprawie przetwarzania […]". (pogrubienie i podkreślenie dodano).

Załącznik
Informacje, które należy przekazać osobie, której dane dotyczą, na podstawie art. 13 lub art. 14

Wymagany rodzaj informacji	Stosowny artykuł (jeśli dane osobowe zostały zebrane bezpośrednio od osoby, której dane dotyczą)	Stosowny artykuł (jeśli dane osobowe nie zostały pozyskane od osoby, której dane dotyczą)	Uwagi GR29 na temat wymogu udzielenia informacji
Tożsamość i dane kontaktowe administratora oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe jego przedstawiciela[59]	Art. 13 ust. 1 lit. a)	Art. 14 ust. 1 lit. a)	Informacje te powinny umożliwiać łatwą identyfikację administratora. Najlepiej byłoby również, gdyby umożliwiały różne formy komunikacji z administratorem danych (np. numer telefonu, adres e-mail, adres korespondencyjny itp.)
Gdy ma to zastosowanie – dane kontaktowe inspektora ochrony danych	Art. 13 ust. 1 lit. b)	Art. 14 ust. 1 lit. b)	Zob. Wytyczne GR29 dotyczące inspektorów ochrony danych[60].
Cele i podstawa prawna przetwarzania	Art. 13 ust. 1 lit. c)	Art. 14 ust. 1 lit. c)	Oprócz określenia celów przetwarzania danych osobowych należy określić stosowną podstawę prawną, na której opiera się przetwarzanie na podstawie art. 6. W przypadku szczególnych kategorii danych osobowych należy określić stosowne przepisy art. 9 (w stosownych | | | przypadkach także mające zastosowanie prawo Unii lub państwa członkowskiego, na mocy którego przetwarza się dane). W przypadku gdy na podstawie art. 10 przetwarza się dane osobowe dotyczące wyroków skazujących oraz naruszeń prawa lub powiązanych środków bezpieczeństwa na podstawie art. 6 ust. 1, w stosownych przypadkach należy określić stosowne prawo Unii lub państwa członkowskiego, na mocy którego dokonuje się przetwarzania.
Jeżeli podstawę prawną przetwarzania stanowią uzasadnione interesy (art. 6 ust. 1 lit. f)) – prawnie uzasadnione interesy realizowane przez administratora danych lub przez stronę trzecią	Art. 13 ust. 1 lit. d)	Art. 14 ust. 2 lit. b)	Odnośny szczególny interes należy określić wobec osoby, której dane dotyczą. W ramach najlepszej praktyki administrator może również przedstawić osobie, której dane dotyczą, informacje uzyskane w wyniku *testu równowagi*, który należy przeprowadzić, aby można było oprzeć się na art. 6 ust. 1 lit. f) jako podstawie prawnej przetwarzania, zanim jakiekolwiek dane osobowe osoby, której dane dotyczą, zostaną zebrane. Aby nie przytłoczyć odbiorcy informacjami, można je włączyć do warstwowego oświadczenia o ochronie prywatności / warstwowej informacji o polityce prywatności (zob. pkt 35). W każdym przypadku stanowisko GR29 jest takie, że z informacji udzielonych osobie, której dane dotyczą, powinno jasno wynikać, iż informacje dotyczące testu równowagi mogą uzyskać na

[59] Jak określono w art. 4 pkt 17 RODO (i o czym mowa w motywie 80), „przedstawiciel" oznacza osobę fizyczną lub prawną mającą miejsce zamieszkania lub siedzibę w UE, która została wyznaczona na piśmie przez administratora lub podmiot przetwarzający na podstawie art. 27 i reprezentuje administratora lub podmiot przetwarzający w zakresie ich obowiązków wynikających z RODO. Obowiązek ten ma zastosowanie w przypadku, gdy zgodnie z art. 3 ust. 2 administrator lub podmiot przetwarzający nie posiada jednostek organizacyjnych w UE, ale przetwarza dane osobowe osób, których dane dotyczą, przebywających w UE, a przetwarzanie wiąże się z oferowaniem towarów lub usług osobom w UE, których dane dotyczą, lub monitorowaniem ich zachowania.

[60] Wytyczne dotyczące inspektorów ochrony danych, GR243 rev.01, ostatnio zmienione i przyjęte w dniu 5 kwietnia 2017 r.

			żądanie. Jest to istotne dla skutecznej przejrzystości w przypadku gdy osoby, których dane dotyczą, mają wątpliwości, czy test równowagi przeprowadzono rzetelnie lub chcą złożyć skargę do organu nadzorczego.
Kategorie odnośnych danych osobowych	Nie jest wymagane	Art. 14 ust. 1 lit. d)	Informacje te są wymagane w ramach scenariusza dotyczącego art. 14, ponieważ dane osobowe nie zostały pozyskane od osoby, której dane dotyczą i która w związku z tym nie wie, jakie kategorie jej danych osobowych pozyskał administrator danych.
Informacje o odbiorcach[61] danych osobowych (lub o kategoriach odbiorców)	Art. 13 ust. 1 lit. e)	Art. 14 ust. 1 lit. e)	Termin „odbiorca" określono w art. 4 pkt 9 jako „osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, **niezależnie od tego, czy jest stroną trzecią**" [pogrubienie dodano] Odbiorca jako taki nie musi być stroną trzecią. W związku z tym termin „odbiorca" obejmuje innych administratorów danych, współadministratorów i podmioty przetwarzające, którym przekazano lub ujawniono dane, a informacje na temat tych odbiorców należy przedstawić dodatkowo do informacji na temat odbiorców będących stronami trzecimi. Należy podać informacje o faktycznych odbiorcach (wymienionych z nazwiska lub nazwy) danych osobowych lub

[61] Określonych w art. 4 pkt 9 RODO i o których mowa w motywie 31

			o kategoriach odbiorców. Zgodnie z zasadą rzetelności administratorzy muszą przedstawić informacje na temat odbiorców, którzy mają największe znaczenie dla osoby, której dane dotyczą. W praktyce zazwyczaj będzie to odbiorca wymieniony z nazwiska lub nazwy, tak aby osoby, których dane dotyczą, wiedziały dokładnie, kto jest w posiadaniu ich danych osobowych. Jeśli administrator zamierza przedstawić kategorie odbiorców, informacje powinny być w jak największym stopniu szczegółowe, tzn. należy wskazać rodzaj odbiorcy (np. poprzez odniesienie do działalności, którą prowadzi), branżę, sektor, podsektor oraz lokalizację odbiorcy.
Szczegóły przekazań do państw trzecich, fakt ich przekazania oraz szczegóły dotyczące stosownych zabezpieczeń[62] (w tym stwierdzenia lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony[63]) oraz możliwości uzyskania kopii danych lub informacje o miejscu udostępnienia danych.	Art. 13 ust. 1 lit. f)	Art. 14 ust. 1 lit. f)	Należy określić stosowny artykuł RODO zezwalający na przekazanie oraz odpowiedni mechanizm (np. decyzja stwierdzająca odpowiedni stopień ochrony na podstawie art. 45 / wiążące reguły korporacyjne na mocy art. 47 / standardowe klauzule ochrony danych na podstawie art. 46 ust. 2 / wyjątki i zabezpieczenia na podstawie art. 49 itd.). Należy również poinformować, gdzie i w jaki sposób można uzyskać dostęp do stosownego dokumentu lub sam dokument, np. podając link do zastosowanego mechanizmu.

[62] Określone w art. 46 ust. 2 i art. 46 ust. 3

[63] Zgodnie z art. 45

			Zgodnie z zasadą rzetelności podane informacje na temat przekazań do państw trzecich powinny być w jak największym stopniu znaczące dla osób, których dane dotyczą, zazwyczaj będzie to oznaczać, że wymieniono nazwę państwa trzeciego.
Okres przechowywania (a gdy nie jest to możliwe, kryteria ustalania tego okresu)	Art. 13 ust. 2 lit. a)	Art. 14 ust. 2 lit. a)	Jest to powiązane z wymogiem dotyczącym minimalizacji danych określonym w art. 5 ust. 1 lit. c) oraz wymogiem w zakresie ograniczenia przechowywania, o którym mowa w art. 5 ust. 1 lit. e). Okres przechowywania (lub kryteria jego ustalania) może być podyktowany takimi czynnikami, jak wymogi ustawowe lub wytyczne branżowe, jednak informacja o nim powinna być sformułowana w taki sposób, aby osoba, której dane dotyczą, miała możliwość ocenienia – na podstawie własnej sytuacji – ile będzie trwał okres zatrzymywania w przypadku określonych danych/celów. Ogólne stwierdzenie przez administratora danych, że dane osobowe będą przechowywane tak długo, jak jest to niezbędne do prawnie uzasadnionych celów przetwarzania, jest niewystarczające. W stosownych przypadkach należy ustalić różne okresy przechowywania dla różnych kategorii danych osobowych lub różnych celów przetwarzania, w tym w stosownych przypadkach, okresy archiwizacji.

Prawa osoby, której dane dotyczą, do: • dostępu; • sprostowania; • usunięcia; • ograniczenia przetwarzania; • sprzeciwu wobec przetwarzania oraz • przenoszenia.	Art. 13 ust. 2 lit. b)	Art. 14 ust. 2 lit. c)	Informacje te powinny być dostosowane do scenariusza przetwarzania oraz zawierać podsumowanie tego, co jest objęte tym prawem, oraz sposobu, w jaki osoba, której dane dotyczą, może podjąć kroki, aby wykonać to prawo, oraz wszelkich ograniczeń tego prawa (zob. pkt 68 powyżej). W szczególności osoba, której dane dotyczą, musi zostać wyraźnie poinformowana o prawie sprzeciwu wobec przetwarzania najpóźniej przy okazji pierwszego kontaktu z taką osobą oraz należy przedstawić jej to prawo jasno i odrębnie od wszelkich innych informacji[64]. W odniesieniu do prawa do przenoszenia zob. Wytyczne GR29 dotyczące prawa do przenoszenia danych[65].
Jeżeli przetwarzanie odbywa się na podstawie zgody (lub wyraźnej zgody), prawo do cofnięcia zgody w dowolnym momencie	Art. 13 ust. 2 lit. c)	Art. 14 ust. 2 lit. d)	Informacja ta powinna obejmować sposób, w jaki można wycofać zgodę, biorąc pod uwagę wymóg, że wycofanie zgody przez osobę, której dane dotyczą, musi być równie łatwe jak jej wyrażenie[66].
Informacje o prawie wniesienia skargi do organu nadzorczego	Art. 13 ust. 2 lit. d)	Art. 14 ust. 2 lit. e)	Informacja ta powinna zawierać wyjaśnienie, że zgodnie z art. 77 osoba, której dane dotyczą, ma prawo wnieść skargę do organu nadzorczego, w szczególności w państwie członkowskim swojego zwykłego pobytu, swojego miejsca pracy lub

[64] Art. 21 ust. 4 oraz motyw 70 (który ma zastosowanie do marketingu bezpośredniego)
[65] Wytyczne dotyczące prawa do przenoszenia danych, GR242 rev.01, ostatnio zmienione i przyjęte w dniu 5 kwietnia 2017 r.
[66] Art. 7 ust. 3

			miejsca popełnienia domniemanego naruszenia RODO.
Informacje o tym, czy istnieje wymóg prawny lub umowny dotyczący przedstawienia informacji, czy przedstawienie informacji jest warunkiem zawarcia umowy lub czy istnieje obowiązek przedstawienia informacji oraz jakie są ewentualne konsekwencje ich nieprzedstawienia.	Art. 13 ust. 2 lit. e)	Nie jest wymagane	Na przykład w kontekście zatrudnienia przedstawienie niektórych informacji obecnemu lub potencjalnemu pracodawcy może stanowić warunek zawarcia umowy. Internetowe formularze powinny wyraźnie określać, które pola są „wymagane", a które nie, oraz jakie będą konsekwencje niewypełnienia wymaganych pól.
Źródło pochodzenia danych osobowych, a gdy ma to zastosowanie – czy pochodzą one ze źródła publicznie dostępnego.	Nie jest wymagane	Art. 14 ust. 2 lit. f)	Należy przedstawić konkretne źródło danych, chyba że jest to niemożliwe – zob. dalsze wskazówki w pkt 60. Jeśli nazwa konkretnego źródła nie została wymieniona, przedstawione informacje powinny obejmować: charakter źródła (tzn. źródło publiczne/prywatne) oraz rodzaj organizacji/branży/sektora.
Informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, oraz – w stosownych przypadkach – istotne informacje o zasadach ich podejmowania oraz o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.	Art. 13 ust. 2 lit. f)	Art. 14 ust. 2 lit. g)	Zob. Wytyczne GR29 w sprawie zautomatyzowanego podejmowania decyzji i profilowania[67].

[67] Wytyczne w sprawie zautomatyzowanego podejmowania decyzji i profilowania do celów rozporządzenia 2016/679, GR 251.

GRUPA ROBOCZA ART. 29

17/PL

WP251rev.01

Wytyczne w sprawie zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania do celów rozporządzenia 2016/679/UE

Przyjęte w dniu 3 października 2017 r.

Ostatnio zmienione i przyjęte w dniu 6 lutego 2018 r.

Grupa Robocza została powołana na mocy art. 29 dyrektywy 95/46/WE. Jest ona niezależnym europejskim organem doradczym w zakresie ochrony danych i prywatności. Zadania Grupy zostały określone w przepisach art. 30 dyrektywy 95/46/WE i art. 15 dyrektywy 2002/58/WE.

Obsługę sekretariatu zapewnia Dyrekcja C (Prawa Podstawowe i Obywatelstwo Unii Europejskiej) Dyrekcji Generalnej ds. Sprawiedliwości Komisji Europejskiej, B-1049 Bruksela, Belgia, biuro nr MO-59 02/013.

Strona internetowa: https://ec.europa.eu/info/law/law-topic/data-protection_pl

GRUPA ROBOCZA DS. OCHRONY OSÓB FIZYCZNYCH W ZAKRESIE

PRZETWARZANIA DANYCH OSOBOWYCH

powołana na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r.,

uwzględniając art. 29 i 30 tej dyrektywy,

uwzględniając swój regulamin wewnętrzny,

PRZYJMUJE NINIEJSZE WYTYCZNE:

SPIS TREŚCI

I. WPROWADZENIE 5

II. DEFINICJE 6

A. Profilowanie 7

B. Zautomatyzowane podejmowanie decyzji 8

C. Jak koncepcje te ujęto w RODO? 9

III. PRZEPISY OGÓLNE DOTYCZĄCE PROFILOWANIA I ZAUTOMATYZOWANEGO PODEJMOWANIA DECYZJI 10

A. Zasady ochrony danych 10

1. Art. 5 ust. 1 lit. a) – Zgodność z prawem, rzetelność i przejrzystość 10

2. Art. 5 ust. 1 lit. b) – Dalsze przetwarzanie i ograniczenie celu 12

3. Art. 5 ust. 1 lit. c) – Minimalizacja danych 12

4. Art. 5 ust. 1 lit. d) – Prawidłowość 13

5. Art. 5 ust. 1 lit. e) – Ograniczenie przechowywania 13

B. Zgodne z prawem podstawy przetwarzania danych 14

1. Art. 6 ust. 1 lit. a) – Zgoda 14

2. Art. 6 ust. 1 lit. b) – Niezbędność do wykonania umowy 14

3. Art. 6 ust. 1 lit. c) – Niezbędność do wypełnienia obowiązku prawnego 15

4. Art. 6 ust. 1 lit. d) – Niezbędność do ochrony żywotnych interesów 15

5. Art. 6 ust. 1 lit. e) – Niezbędność do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej 16

6. Art. 6 ust. 1 lit. f) – Niezbędność do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub stronę trzecią 16

C. Art. 9 – Szczególne kategorie danych osobowych 17

D. Prawa osoby, której dane dotyczą 17

1. Art. 13 i 14 – Prawo do otrzymania informacji 18

2. Art. 15 – Prawo dostępu 19

3. Art. 16 – Prawo do sprostowania danych, art. 17 – Prawo do usunięcia danych oraz art. 18 – Prawo do ograniczenia przetwarzania 20

4. Art. 21 – Prawo do sprzeciwu 20

IV. PRZEPISY SZCZEGÓLNE DOTYCZĄCE PODEJMOWANIA DECYZJI WYŁĄCZNIE W SPOSÓB ZAUTOMATYZOWANY ZAWARTE W ART. 22 22

A. „Decyzja, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu" 23

B. „Skutki prawne" lub „podobny istotny wpływ" 24

C. Wyjątki od zakazu 26

1. Wykonanie umowy 26

2. Dopuszczenie prawem Unii lub prawem państwa członkowskiego *27*

3. Wyraźna zgoda *27*

D. SZCZEGÓLNE KATEGORIE DANYCH OSOBOWYCH – ART. 22 UST. 4 27

E. PRAWA OSOBY, KTÓREJ DANE DOTYCZĄ 28

1. Art. 13 ust. 2 lit. f) i art. 14 ust. 2 lit. g) – Prawo do otrzymania informacji *28*

2. Art. 15 ust. 1 lit. h) – Prawo dostępu *30*

F. USTANAWIANIE ODPOWIEDNICH ZABEZPIECZEŃ 31

V. DZIECI A PROFILOWANIE 32

VI. OCENA SKUTKÓW DLA OCHRONY DANYCH I INSPEKTOR OCHRONY DANYCH 34

ZAŁĄCZNIK 1 – ZALECENIA W ZAKRESIE DOBRYCH PRAKTYK 35

ZAŁĄCZNIK 2 – KLUCZOWE PRZEPISY RODO 38

KLUCZOWE PRZEPISY RODO ODNOSZĄCE SIĘ DO PROFILOWANIA DO CELÓW OGÓLNYCH I ZAUTOMATYZOWANEGO PODEJMOWANIA DECYZJI 38

KLUCZOWE PRZEPISY RODO ODNOSZĄCE SIĘ DO ZAUTOMATYZOWANEGO PODEJMOWANIA DECYZJI W ROZUMIENIU ART. 22..... 39

ZAŁĄCZNIK 3 – MATERIAŁY UZUPEŁNIAJĄCE 42

I. Wprowadzenie

Ogólne rozporządzenie o ochronie danych (RODO) odnosi się konkretnie do kwestii profilowania i zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach, w tym profilowania[1].

Profilowanie i zautomatyzowanie podejmowanie decyzji wykorzystuje się w coraz liczniejszych sektorach, zarówno prywatnych, jak i publicznych. Bankowość i finanse, opieka zdrowotna, podatki, ubezpieczenia, marketing i reklamy to jedynie kilka przykładów obszarów, w których coraz częściej przy podejmowaniu decyzji wykorzystuje się profilowanie.

Za sprawą postępu technicznego i zdolności w zakresie analizowania dużych zbiorów danych, sztucznej inteligencji i uczenia się maszyn tworzenie profili i podejmowanie zautomatyzowanych decyzji jest coraz łatwiejsze i potencjalnie może w znacznym stopniu wpływać na prawa i wolności osób fizycznych.

Powszechna dostępność danych osobowych w internecie i za pośrednictwem urządzeń internetu rzeczy (IoT) oraz zdolność do wyszukiwania korelacji i tworzenia powiązań sprawiają, że możliwe staje się określanie, analizowanie i przewidywanie różnych aspektów osobowości lub zachowania osób fizycznych.

Profilowanie i zautomatyzowane podejmowanie decyzji mogą stanowić przydatne narzędzia dla osób fizycznych i organizacji, przynosząc takie korzyści, jak:

- większa wydajność oraz
- oszczędność zasobów.

Procesy te mają wiele zastosowań komercyjnych, przykładowo mogą być wykorzystywane do lepszego dzielenia rynków na segmenty oraz dostosowywania ofert i produktów do indywidualnych potrzeb. Mogą przynosić korzyści również w medycynie, edukacji i transporcie.

Profilowanie i zautomatyzowane podejmowanie decyzji mogą jednak stwarzać znaczne zagrożenie dla praw i wolności osób fizycznych, przez co konieczne jest zapewnienie odpowiednich zabezpieczeń.

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE. Profilowanie i zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach to zagadnienia objęte również zakresem stosowania dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych. Choć w niniejszych wytycznych skoncentrowano się na profilowaniu i zautomatyzowanym podejmowaniu decyzji w indywidualnych przypadkach, o których mowa w RODO, mają one również zastosowanie w odniesieniu do podobnych przepisów dyrektywy 2016/680 dotyczących tych dwóch zagadnień. Niniejsze wytyczne nie obejmują analizy specyfiki profilowania i zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach w kontekście dyrektywy 2016/680, gdyż wytyczne w tym zakresie zostały przedstawione w opinii WP 258 dotyczącej kluczowych elementów dyrektywy ((UE) 2016/680) dotyczącej egzekwowania prawa, przyjętej przez Grupę Roboczą Art. 29 w dniu 29 listopada 2017 r. Opinia ta obejmuje kwestie zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania w kontekście przetwarzania danych do celów egzekwowania prawa (s. 11–14) i jest dostępna pod adresem: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610178

Procesy te bywają nieprzejrzyste. Osoby fizyczne mogą nie wiedzieć, że są profilowane, lub mogą nie wiedzieć, co się z tym wiąże.

Profilowanie może utrwalać istniejące stereotypy i segregację społeczną. Może również skutkować zamykaniem osób w konkretnej kategorii i traktowaniem ich wyłącznie z uwzględnieniem sugerowanych preferencji. Może to powodować m.in. ograniczenie ich wolności wyboru określonych produktów lub usług, jak np. książki, muzyka czy też najnowsze wiadomości. W niektórych przypadkach przewidywanie przy użyciu profilowania może dawać nieprawidłowe wyniki. W innych przypadkach profilowanie może skutkować odmową świadczenia usług i dostarczenia towarów oraz nieuzasadnioną dyskryminacją.

W RODO wprowadzono nowe przepisy w celu wyeliminowania ryzyka wynikającego z profilowania i zautomatyzowanego podejmowania decyzji – w szczególności, choć nie wyłącznie, ryzyka naruszenia prawa do prywatności. Celem niniejszych wytycznych jest wyjaśnienie takich przepisów.

W niniejszym dokumencie przedstawiono następujące zagadnienia:

- definicje profilowania i zautomatyzowanego podejmowania decyzji oraz ogólne podejście do tych kwestii przyjęte w RODO – rozdział II;
- przepisy ogólne dotyczące profilowania i zautomatyzowanego podejmowania decyzji – rozdział III;
- przepisy szczególne dotyczące podejmowania decyzji wyłącznie w sposób zautomatyzowany zawarte w art. 22 – rozdział IV;
- dzieci a profilowanie – rozdział V;
- oceny skutków dla ochrony danych i inspektorzy ochrony danych – rozdział VI.

W załącznikach przedstawiono zalecenia dotyczące najlepszych praktyk, które opracowano w oparciu o doświadczenia zgromadzone w państwach członkowskich UE.

Grupa Robocza ds. Ochrony Osób Fizycznych w zakresie Przetwarzania Danych Osobowych (Grupa Robocza Art. 29) będzie monitorowała wdrażanie niniejszych wytycznych i może w stosownych przypadkach uzupełnić je o dodatkowe informacje.

II. Definicje

W RODO wprowadzono przepisy mające na celu zapewnienie, aby profilowanie i zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach (niezależnie od tego, czy takie podejmowanie decyzji obejmuje profilowanie, czy też nie) wykorzystywano w sposób niewywierający nieuzasadnionego wpływu na prawa osób fizycznych. Takie przepisy obejmują na przykład:

- szczególne wymogi dotyczące przejrzystości i rzetelności;
- zaostrzenie obowiązków w zakresie rozliczalności;
- określenie podstaw prawnych przetwarzania;
- prawa osób fizycznych do sprzeciwu wobec profilowania, a w szczególności profilowania do celów marketingu; oraz
- konieczność przeprowadzenia w określonych warunkach oceny skutków dla ochrony danych.

W RODO nie skoncentrowano się wyłącznie na decyzjach podejmowanych w wyniku zautomatyzowanego przetwarzania lub profilowania. RODO ma zastosowanie do zbierania danych do celów tworzenia profili oraz stosowania tych profili w odniesieniu do osób fizycznych.

A. Profilowanie

Art. 4 pkt 4 RODO zawiera następującą definicję terminu „profilowanie":

> dowolna forma zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.

Profilowanie składa się z trzech elementów:

- profilowanie musi stanowić *zautomatyzowaną* formę przetwarzania;
- profilowaniu muszą podlegać *dane osobowe*; oraz
- celem profilowania musi być *ocena czynników osobowych osób fizycznych*.

W art. 4 pkt 4 jest mowa o „dowolnej formie zautomatyzowanego przetwarzania", a nie o „wyłącznie" zautomatyzowanym przetwarzaniu (o którym mowa w art. 22). Profilowanie musi obejmować pewną formę zautomatyzowanego przetwarzania – interwencja ludzka nie musi jednak powodować, że dane działanie wykracza poza definicję profilowania.

Profilowanie to procedura, która może obejmować szereg wniosków na podstawie przesłanek statystycznych. Technikę tę często stosuje się do tworzenia prognoz na temat osób fizycznych. Dane z różnych źródeł wykorzystuje się do wyciągania wniosków na temat danej osoby na podstawie cech innych osób, do których dana osoba ze statystycznego punktu widzenia wydaje się podobna.

RODO stanowi, że profilowanie to zautomatyzowane przetwarzanie danych osobowych do oceny czynników osobowych, w szczególności do analizy *lub* prognozy aspektów dotyczących osób fizycznych. Użycie słowa „ocena" sugeruje, że profilowanie obejmuje pewną formę oceny lub osądu danej osoby.

Zwykła klasyfikacja osób fizycznych ze względu na znane cechy, jak np. wiek, płeć i wzrost, nie musi skutkować profilowaniem. Decydujący będzie cel takiej klasyfikacji.
Przykładowo, klasyfikując swoich klientów ze względu na wiek lub płeć, przedsiębiorstwo może kierować się względami statystycznymi, chcąc uzyskać zbiorczy przegląd klientów bez prognozowania lub wyciągania wniosków na temat konkretnej osoby fizycznej. W takim przypadku celem nie jest ocena cech danej osoby fizycznej, a zatem nie ma mowy o profilowaniu.

Definicja zawarta w RODO opiera się na definicji profilowania określonej w zaleceniu Rady Europy (2010)13[2] („zalecenie"), choć nie jest identyczna. Zalecenie Rady Europy *wyklucza* przetwarzanie nieobejmujące wnioskowania. Zawiera jednak przydatne wyjaśnienie, zgodnie z którym profilowanie może obejmować trzy różne etapy:

- zbieranie danych;

[2] Rada Europy, „The protection of individuals with regard to automatic processing of personal data in the context of profiling" [„Ochrona osób w związku z automatycznym przetwarzaniem danych osobowych w kontekście profilowania"]. Zalecenie CM/Rec(2010)13 wraz z uzasadnieniem. Rada Europy, dnia 23 listopada 2010 r. https://www.coe.int/t/dghl/standardsetting/cdcj/CDCJ%20Recommendations/CMRec(2010)13E_Profiling.pdf. Data uzyskania dostępu: 24 kwietnia 2017 r.

- zautomatyzowaną analizę w celu określenia korelacji;
- wykorzystywanie korelacji do celów stworzenia charakterystyki obecnego lub przyszłego zachowania danej osoby fizycznej.

Administratorzy prowadzący profilowanie będą musieli zapewnić przestrzeganie wymogów określonych w RODO w odniesieniu do wszystkich wyżej wymienionych etapów.

Zasadniczo profilowanie oznacza gromadzenie informacji o danej osobie (lub grupie osób fizycznych) i ocenę ich cech lub wzorców zachowania w celu zakwalifikowania ich do określonej kategorii lub grupy, w szczególności do celów analizy lub prognozy takich aspektów, jak wykazywane przez dane osoby:

- zdolności do wykonania danego zadania;
- zainteresowania; lub
- prawdopodobne zachowania.

Przykład

Broker informacji zbiera dane z różnych źródeł publicznych i prywatnych w imieniu swoich klientów albo do własnych celów. Następnie zestawia dane w celu stworzenia profili osób fizycznych i dzieli je na segmenty. Informacje te sprzedaje przedsiębiorstwom, które pragną, aby ich towary i usługi były lepiej ukierunkowane. Broker informacji profiluje daną osobę, klasyfikując ją do określonej kategorii na podstawie jej zainteresowań.

Występowanie zautomatyzowanego podejmowania decyzji zdefiniowanego w art. 22 ust. 1 będzie zależało od okoliczności.

B. Zautomatyzowane podejmowanie decyzji

Zautomatyzowane podejmowanie decyzji ma inny zakres niż profilowanie, może jednak częściowo pokrywać się z profilowaniem lub z niego wynikać. Podejmowanie decyzji wyłącznie w sposób zautomatyzowany to zdolność do podejmowania decyzji z wykorzystaniem rozwiązań technicznych bez interwencji ludzkiej. Zautomatyzowane decyzje mogą być podejmowane w oparciu o wszelkiego rodzaju dane, w tym na przykład:

- dane przekazane bezpośrednio przez zainteresowane osoby fizyczne (np. respondentów wypełniających kwestionariusz);
- dane zaobserwowane na temat osób fizycznych (np. dane o lokalizacji zbierane za pośrednictwem aplikacji);
- dane pochodne lub wywnioskowane, na przykład profil osoby fizycznej, który został już utworzony (np. punktowa ocena kredytowa).

Zautomatyzowane podejmowanie decyzji może, ale nie musi, obejmować profilowanie, z kolei profilowanie może zachodzić bez podejmowania zautomatyzowanych decyzji. Profilowanie i zautomatyzowane podejmowanie decyzji nie muszą jednak stanowić odrębnych działań. Bywa, że działanie, które początkowo stanowi zwykły proces zautomatyzowanego podejmowania decyzji, może

przekształcić się w działanie oparte na profilowaniu, co będzie zależeć od sposobu wykorzystania danych.

Przykład

Nakładanie mandatów za przekroczenie dozwolonej prędkości na podstawie dowodów z fotoradarów to proces zautomatyzowanego podejmowania decyzji, który nie musi obejmować profilowania.

Podjęta w ten sposób decyzja stałaby się jednak decyzją opartą na profilowaniu, jeżeli monitorowano by przez pewien czas zachowania danej osoby fizycznej jako kierowcy, i, przykładowo, wysokość nałożonego mandatu uzależniona byłaby od oceny uwzględniającej inne czynniki, takie jak kwestia, czy wcześniej dana osoba przekraczała już prędkość lub czy w ostatnim czasie w inny sposób naruszała przepisy prawa drogowego.

Decyzje, które nie opierają się wyłącznie na zautomatyzowanym przetwarzaniu, również mogą obejmować profilowanie. Przykładowo przed udzieleniem kredytu hipotecznego bank może analizować punktową ocenę kredytową kredytobiorcy, co może obejmować dodatkową znaczącą interwencję ludzką przed wydaniem decyzji wobec danej osoby fizycznej.

C. Jak koncepcje te ujęto w RODO?

Istnieją trzy możliwe sposoby stosowania profilowania:

(i) profilowanie do celów ogólnych;
(ii) podejmowanie decyzji na podstawie profilowania; oraz
(iii) podejmowanie decyzji *wyłącznie* w sposób zautomatyzowany, w tym profilowanie, wywołujące wobec osoby, której dane dotyczą, skutki prawne lub w podobny sposób istotnie na nią wpływające (art. 22 ust. 1).

Różnicę między przypadkami w pkt (ii) i (iii) najlepiej ilustrują dwa poniższe przykłady, w których osoba fizyczna składa wniosek o kredyt przez internet:

- decyzja w sprawie udzielenia kredytu jest podejmowana przez człowieka na podstawie profilu utworzonego wyłącznie za pomocą środków zautomatyzowanych (ii);
- decyzja w sprawie udzielenia kredytu jest podejmowana za pomocą algorytmu i automatycznie przekazywana danej osobie fizycznej, której dotyczy, nie podlegając wcześniej żadnej znaczącej ocenie przez człowieka (iii).

Administratorzy mogą stosować profilowanie i zautomatyzowane podejmowanie decyzji pod warunkiem, że przestrzegają wszystkich zasad, a przetwarzanie danych odbywa się zgodnie z określoną podstawą prawną. W przypadku podejmowania decyzji wyłącznie w sposób zautomatyzowany, w tym w oparciu o profilowanie w rozumieniu art. 22 ust. 1, zastosowanie mają dodatkowe zabezpieczenia i ograniczenia.

Rozdział III niniejszych wytycznych zawiera objaśnienie przepisów RODO w zakresie *wszystkich* przypadków profilowania i zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach. Dotyczy to również procesów decyzyjnych, które *nie* przebiegają wyłącznie w sposób zautomatyzowany.

Rozdział IV niniejszych wytycznych zawiera objaśnienia przepisów szczególnych, które mają zastosowanie *wyłącznie* do podejmowania decyzji w indywidualnych przypadkach w sposób

całkowicie zautomatyzowany, w tym profilowania[3]. Obowiązuje ogólny zakaz stosowania takiego rodzaju przetwarzania, wynikający z potencjalnych zagrożeń dla praw i wolności osób fizycznych.

III. Przepisy ogólne dotyczące profilowania i zautomatyzowanego podejmowania decyzji

Przedstawiony tu przegląd przepisów obejmuje wszystkie przypadki profilowania i zautomatyzowanego podejmowania decyzji. Dodatkowe przepisy szczególne określone w rozdziale IV mają zastosowanie, jeżeli przetwarzanie spełnia definicję określoną w art. 22 ust. 1.

A. Zasady ochrony danych

Zasady te mają zastosowanie we wszystkich przypadkach profilowania i zautomatyzowanego podejmowania decyzji z wykorzystaniem danych osobowych[4]. Aby łatwiej było zachować zgodność z przepisami, administratorzy powinni rozważyć następujące kluczowe obszary:

1. Art. 5 ust. 1 lit. a) – Zgodność z prawem, rzetelność i przejrzystość

Przejrzystość przetwarzania to jeden z podstawowych wymogów ujętych w RODO[5].

Proces profilowania często jest niewidoczny dla osoby, której dane dotyczą. Proces ten polega na tworzeniu danych pochodnych lub wywnioskowanych na temat osób fizycznych – „nowych" danych osobowych, które nie zostały przekazane bezpośrednio przez same osoby, których dane dotyczą. Osoby fizyczne wykazują różny poziom zrozumienia i mogą mieć trudność ze zrozumieniem złożonych technik stosowanych w ramach procesów profilowania i zautomatyzowanego podejmowania decyzji.

Zgodnie z art. 12 ust. 1 administrator musi w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie udzielić osobie, której dane dotyczą, informacji na temat przetwarzania ich danych osobowych[6].

[3] W rozumieniu art. 22 ust. 1 RODO.

[4] RODO – motyw 72 „Profilowanie podlega przepisom niniejszego rozporządzenia dotyczącym przetwarzania danych osobowych, takim jak przepisy określające podstawy prawne przetwarzania lub zasady ochrony danych".

[5] Szczegółowe informacje na temat przejrzystości można znaleźć w dokumencie: Grupa Robocza Art. 29, „Wytyczne dotyczące przejrzystości na mocy rozporządzenia 2016/679" (WP 260 rev.01), 11 kwietnia 2018 r., http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227

[6] Office of the Australian Information Commissioner [Biuro Australijskiego Komisarza ds. Informacji]. „Consultation draft: Guide to big data and the Australian Privacy Principles" [„Projekt do konsultacji: Wytyczne w sprawie dużych zbiorów danych w kontekście australijskich zasady ochrony prywatności"], maj 2016 r.: „Informacje o polityce prywatności muszą przedstawiać praktyki w zakresie przetwarzania danych w sposób jasny i prosty, a jednocześnie kompleksowy i na tyle szczegółowy, aby były rzetelne. Ta sama technologia, która powoduje zbieranie większych ilości danych osobowych, może być wykorzystywana do tego, aby informacje o polityce prywatności były bardziej dynamiczne, wielopoziomowe i ukierunkowane na użytkownika". https://www.oaic.gov.au/engage-with-us/consultations/guide-to-big-data-and-the-australian-privacy-principles/consultation-draft-guide-to-big-data-and-the-australian-privacy-principles. Data uzyskania dostępu: 24 kwietnia 2017 r.

Jeżeli dane zbierane są bezpośrednio od osoby, której dotyczą, informacje te należy podać podczas pozyskiwania takich danych (art. 13), natomiast w przypadku danych uzyskanych pośrednio informacje o polityce prywatności należy podać z zachowaniem terminów określonych w art. 14 ust. 3.

Przykład

Niektórzy ubezpieczyciele oferują stawki i usługi ubezpieczeniowe na podstawie zachowania danej osoby fizycznej jako kierowcy. W takich przypadkach mogą być uwzględniane takie elementy, jak: przebyty dystans, czas podróży i przebyte trasy oraz prognozy opierające się na innych danych zebranych przez czujniki znajdujące się w (inteligentnym) samochodzie. Zebrane dane wykorzystuje się do profilowania celem identyfikacji złych zachowań kierowcy (takich jak szybkie przyspieszanie, nagłe hamowanie i przekraczanie dozwolonej prędkości). Takie informacje mogą zostać zestawione z innymi źródłami (zawierającymi np. dane dotyczące pogody, natężenia ruchu, rodzaju drogi), aby zapewnić możliwość lepszego zrozumienia zachowania kierowcy.

Administrator musi upewnić się, że dysponuje podstawą prawną uzasadniającą ten rodzaj przetwarzania. Administrator musi również poinformować osobę, której dane dotyczą, o zebranych danych oraz – w stosownych przypadkach – o stosowaniu zautomatyzowanego podejmowania decyzji, o którym mowa w art. 22 ust. 1 i 4, o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania.

Konkretne wymogi regulujące kwestie związane z informacjami i dostępem do danych osobowych zostały omówione w rozdziałach III (sekcja D) i IV (sekcja E).

Przetwarzanie danych musi również odbywać się w sposób rzetelny i przejrzysty.

Profilowanie może odbywać się w sposób nierzetelny i prowadzić do dyskryminacji polegającej np. na odmawianiu osobom dostępu do zatrudnienia, możliwości zaciągnięcia kredytu lub wykupienia ubezpieczenia lub oferowaniu im zbyt ryzykownych lub kosztownych produktów finansowych. Poniższy przykład, który nie spełniłby wymogów ustanowionych w art. 5 ust. 1 lit. a), pokazuje, w jaki sposób nierzetelne profilowanie może doprowadzić do sytuacji, w której niektórzy konsumenci będą otrzymywać mniej atrakcyjne oferty niż inni.

Przykład

Broker informacji sprzedaje profile konsumentów spółkom finansowym bez zgody konsumenta lub bez zapoznania się z danymi bazowymi. Na podstawie sporządzonych profili konsumentów dzieli się na kategorie (noszące nazwy takie jak „mieszkaniec wsi ledwo wiążący koniec z końcem", „borykający się z problemami finansowymi mieszkaniec średniej wielkości miasta należący do mniejszości etnicznej", „trudny początek: młodzi samotni rodzice") lub przyznaje się im punkty w zależności od poziomu niestabilności ich sytuacji finansowej. Następnie spółki finansowe oferują tym konsumentom chwilówki i inne „niekonwencjonalne" usługi finansowe (wysoko oprocentowane pożyczki i inne produkty wiążące się z ryzykiem finansowym)[7].

[7] Opisany przykład zaczerpnięto z: Senat Stanów Zjednoczonych, Komisja ds. Handlu, Nauki i Transportu. „A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes, Staff Report for Chairman Rockefeller" [„Przegląd działalności brokerów informacji: gromadzenie, wykorzystywanie i sprzedaż danych konsumentów do celów marketingowych – sprawozdanie służb dla przewodniczącego Rockefellera"], 18 grudnia 2013 r. https://www.commerce.senate.gov/public/_cache/files/0d2b3642-6221-4888-a631-08f2f255b577/AE5D72CBE7F44F5BFC846BECE22C875B.12.18.13-senate-commerce-committee-report-on-data-broker-industry.pdf. Zob. w szczególności s. ii streszczenia i s. 12 głównej części dokumentu. Data uzyskania dostępu: 21 lipca 2017 r.

2. Art. 5 ust. 1 lit. b) – Dalsze przetwarzanie i ograniczenie celu

Profilowanie może wiązać się z wykorzystywaniem danych osobowych, które pierwotnie zebrano w innym celu.

Przykład

Niektóre aplikacje mobilne zapewniają użytkownikowi możliwość korzystania z usług lokalizacji, aby ułatwić mu znalezienie pobliskich restauracji oferujących zniżki. Zbierane w ten sposób dane są jednak wykorzystywane również do tworzenia profilu osoby, której dane dotyczą, do celów marketingowych – tj. do ustalenia jej preferencji żywieniowych lub ogólnie rozumianego stylu życia. Osoba, której dane dotyczą, spodziewa się, że jej dane będą wykorzystywane do wyszukiwania restauracji, ale nie do przesyłania jej reklam usług dowozu pizzy wyłącznie z uwagi na fakt, że aplikacja rozpoznała, że osoba ta późno wraca do domu. Takie dodatkowe wykorzystywanie danych dotyczących lokalizacji może być niezgodne z celami, dla których pierwotnie zebrano te dane, dlatego też może wiązać się z koniecznością uzyskania zgody danej osoby[8].

To, czy takie dodatkowe przetwarzanie jest zgodne z pierwotnymi celami, dla których dane zostały zebrane, będzie zależało od szeregu czynników[9], m.in. od tego, jakich informacji administrator udzielił początkowo osobie, której dane dotyczą. Wspomniane czynniki zostały uwzględnione w RODO[10] – poniżej przedstawiono ich streszczenie:

- związek między celami, dla których zbierano dane, a celami ich dalszego przetwarzania;
- kontekst, w którym zbierano dane, oraz uzasadnione oczekiwania ze strony osób, których dane dotyczą, co do ich dalszego wykorzystywania;
- charakter danych;
- wpływ dalszego przetwarzania na osoby, których dane dotyczą; oraz
- zabezpieczenia przyjęte przez administratora w celu zapewnienia przetwarzania danych w rzetelny sposób i zapobieżenia wszelkiemu niepożądanemu wpływowi takiego przetwarzania na osoby, których dane dotyczą.

3. Art. 5 ust. 1 lit. c) – Minimalizacja danych

Możliwości rynkowe wynikające z profilowania, niższych kosztów przechowywania oraz możliwości przetwarzania dużych ilości informacji mogą zachęcić organizacje do zbierania większej ilości danych osobowych niż ilość, która jest im faktycznie potrzebna – do ewentualnego wykorzystania w przyszłości. Administratorzy muszą zapewnić przestrzeganie zasad minimalizacji danych, a także wymogów w zakresie ograniczenia celu i ograniczenia przechowywania.

[8] Należy zwrócić uwagę na fakt, że w takim przypadku zastosowanie mogą mieć również przepisy rozporządzenia w sprawie prywatności i łączności elektronicznej, które ma zostać przyjęte w przyszłości.

[9] Grupa Robocza Art. 29 zwróciła na to uwagę w swojej opinii nr 03/2013 w sprawie ograniczenia celu przyjętej w dniu 2 kwietnia 2013 r. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf . Data uzyskania dostępu: 24 kwietnia 2017 r.

[10] Art. 6 ust. 4 RODO.

Administratorzy powinni być w stanie w przejrzysty sposób wyjaśnić i uzasadnić konieczność zbierania i przechowywania danych osobowych lub powinni rozważyć możliwość korzystania do celów profilowania z danych zagregowanych, danych zanonimizowanych lub (w przypadku zapewnienia wystarczającego poziomu ochrony) danych poddanych pseudonimizacji.

4. Art. 5 ust. 1 lit. d) – Prawidłowość

Administratorzy powinni brać pod uwagę kwestie związane z prawidłowością danych na wszystkich etapach procesu profilowania, a w szczególności przy:

- zbieraniu danych;
- analizowaniu danych;
- tworzeniu profilu danej osoby fizycznej; lub
- wykorzystywaniu profilu do podjęcia decyzji wywierającej wpływ na daną osobę fizyczną.

Jeżeli dane wykorzystywane w procesie zautomatyzowanego podejmowania decyzji lub profilowania okażą się nieprawidłowe, wszelkie decyzje podjęte w oparciu o te dane lub wszelkie profile sporządzone na podstawie tych danych będą wadliwe. Może to skutkować podejmowaniem decyzji na podstawie nieaktualnych danych lub niewłaściwej interpretacji danych zewnętrznych. Nieprawidłowości mogą doprowadzić do nietrafnych przewidywań lub deklaracji dotyczących np. stanu zdrowia danej osoby lub poziomu ryzyka kredytowego lub ubezpieczeniowego, na jakie jest ona narażona.

Nawet w przypadku prawidłowego zarejestrowania surowych danych zbiory danych mogą nie być w pełni reprezentatywne lub analizy mogą zawierać ukryty element stronniczości.

Administratorzy muszą wprowadzać skuteczne środki zapewniające możliwość bieżącego monitorowania i zapewnienia prawidłowości i aktualności ponownie wykorzystywanych danych lub danych pozyskanych pośrednio. Tym ważniejsze jest udzielanie przejrzystych informacji na temat przetwarzanych danych osobowych, aby osoba, której dane dotyczą, mogła skorygować wszelkie nieprawidłowości, zwiększając tym samym jakość danych.

5. Art. 5 ust. 1 lit. e) – Ograniczenie przechowywania

Algorytmy uczenia się maszyn opracowuje się z myślą o przetwarzaniu dużych ilości informacji i budowaniu korelacji umożliwiających organizacjom tworzenie bardzo złożonych, intymnych profili osób fizycznych. Choć przechowywanie danych może wiązać się z korzyściami w kontekście profilowania, ponieważ zapewnia dostęp do większej ilości danych, które algorytm może wykorzystać do uczenia się, administratorzy muszą przy zbieraniu danych osobowych przestrzegać zasady minimalizacji danych oraz przechowywać takie dane osobowe wyłącznie na czas konieczny do osiągnięcia celów, w jakich przetwarza się te dane osobowe, i w sposób proporcjonalny do tych celów.

W stosowanej przez siebie polityce przechowywania danych administrator powinien wziąć pod uwagę prawa i wolności osób fizycznych zgodnie z wymogami art. 5 ust. 1 lit. e).

Administrator powinien również zapewnić aktualizację danych przez cały okres zatrzymywania, aby ograniczyć ryzyko wystąpienia nieprawidłowości[11].

[11] Norweski organ ochrony danych, „The Great Data Race – How commercial utilisation of personal data challenges privacy" [„W pogoni za danymi – Zagrożenie dla prywatności, jakie niesie ze sobą wykorzystywanie danych osobowych do celów komercyjnych"], sprawozdanie, listopad 2015. Datatilsynet https://www.datatilsynet.no/English/Publications/The-Great-Data-Race/. Data uzyskania dostępu: 24 kwietnia

B. Zgodne z prawem podstawy przetwarzania danych

Z procesu zautomatyzowanego podejmowania decyzji, o którym mowa w art. 22 ust. 1, można korzystać wyłącznie w przypadku, gdy zastosowanie ma jeden z wyjątków opisanych w rozdziale IV (sekcje C i D). Przedstawione poniżej zgodne z prawem podstawy przetwarzania mają zastosowanie we wszystkich innych sytuacjach, w których dochodzi do zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania.

1. Art. 6 ust. 1 lit. a) – Zgoda

Kwestie odnoszące się do zgody jako ogólnej podstawy uprawniającej do przetwarzania danych zostały zasadniczo omówione w wytycznych Grupy Roboczej Art. 29 dotyczących zgody[12]. Udzielenie wyraźnej zgody stanowi jeden z wyjątków od zakazu zautomatyzowanego podejmowania decyzji i profilowania ustanowionego w art. 22 ust. 1.

Proces profilowania może przebiegać w sposób nieprzejrzysty. W ramach tego procesu często wykorzystuje się dane wywodzące się lub wywnioskowane z innych danych, a nie dane bezpośrednio przekazane przez osobę, której dotyczą.

Administratorzy chcący oprzeć się na zgodzie jako podstawie uzasadniającej profilowanie będą musieli wykazać, że osoby, których dane dotyczą, dobrze rozumieją, na co dokładnie się zgadzają, a także pamiętać o tym, że zgoda nie zawsze stanowi odpowiednią podstawę uzasadniającą przetwarzanie danych[13]. Niezależnie od danego przypadku osoby, których dane dotyczą, powinny dysponować odpowiednią ilością stosownych informacji na temat planowanego wykorzystania danych oraz konsekwencji związanych z ich przetwarzaniem, tak aby wyrażona przez nie zgoda wynikała z ich świadomej decyzji.

2. Art. 6 ust. 1 lit. b) – Niezbędność do wykonania umowy

Administratorzy mogą chcieć korzystać z procesów profilowania i zautomatyzowanego podejmowania decyzji, ponieważ procesy te:

- mogą potencjalnie zapewnić większą spójność lub rzetelność procesu podejmowania decyzji (np. dzięki ograniczeniu możliwości wystąpienia błędu ludzkiego, a także przypadków dyskryminacji i nadużycia władzy);
- ograniczają ryzyko nieuiszczenia płatności za towary lub usługi przez klientów (na przykład dzięki korzystaniu z zasobów informacji kredytowych); lub
- zapewniają administratorom możliwość szybszego wydawania decyzji i sprawniejszego działania.

2017 r.[12] Grupa Robocza Art. 29, „Wytyczne dotyczące zgody na mocy rozporządzenia 2016/679", WP259, 28 listopada 2017 r., http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48849 . Data uzyskania dostępu: 18 grudnia 2017 r.

[12] Grupa Robocza Art. 29, „Wytyczne dotyczące zgody na mocy rozporządzenia 2016/679", WP259, 28 listopada 2017 r., http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48849 . Data uzyskania dostępu: 18 grudnia 2017 r.

[13] *Ibidem.*

Niemniej jednak wymienione powyżej powody same w sobie nie stanowią wystarczającej podstawy do tego, by wykazać, że taki rodzaj przetwarzania jest *niezbędny* do wykonania umowy w rozumieniu art. 6 ust. 1 lit. b). Jak opisano w opinii Grupy Roboczej Art. 29 dotyczącej uzasadnionego interesu[14], pojęcie niezbędności powinno się interpretować wąsko.

Poniżej przedstawiono przykład profilowania, które *nie* spełniałoby ustanowionych w art. 6 ust. 1 lit. b) warunków uznania przetwarzania za zgodne z prawem.

Przykład

Użytkownik kupuje określone przedmioty w sklepie internetowym. Aby wywiązać się z umowy, sklep musi przetwarzać informacje z karty kredytowej użytkownika do celów związanych z realizacją płatności oraz dane adresowe użytkownika w celu dostarczenia mu towarów. Możliwość wywiązania się z umowy nie zależy od stworzenia profilu preferencji i stylu życia użytkownika na podstawie historii jego wejść na stronę internetową. Nawet jeżeli w warunkach umowy zawarto klauzulę wyraźnie informującą o możliwości stosowania profilowania, sam fakt zawarcia takiej klauzuli nie sprawia, że profilowanie staje się „niezbędne" do wykonania umowy.

3. Art. 6 ust. 1 lit. c) – Niezbędność do wypełnienia obowiązku prawnego

W niektórych przypadkach konieczność profilowania wynika z określonego obowiązku prawnego[15] – na przykład w kontekście zapobiegania oszustwom lub przeciwdziałania praniu pieniędzy. W opinii Grupy Roboczej Art. 29 dotyczącej uzasadnionych interesów[16] zawarto przydatne informacje na temat tej podstawy przetwarzania, w tym informacje na temat zabezpieczeń, które należy stosować.

4. Art. 6 ust. 1 lit. d) – Niezbędność do ochrony żywotnych interesów

Przepisy art. 6 ust. 1 lit. d) odnoszą się do sytuacji, w których przetwarzanie jest niezbędne do ochrony interesu mającego istotne znaczenie dla życia osoby, której dane dotyczą, lub innej osoby fizycznej.

Niektóre rodzaje przetwarzania mogą służyć ochronie ważnych interesów publicznych i żywotnych interesów osoby, której dane dotyczą. Wśród przykładów takich rodzajów przetwarzania można wymienić profilowanie konieczne do opracowania modeli pozwalających przewidzieć ścieżkę rozprzestrzeniania się chorób zagrażających życiu lub profilowanie przeprowadzane w nadzwyczajnych sytuacjach humanitarnych. Jednak w takich sytuacjach – i co do zasady – administrator może powołać się na konieczność ochrony żywotnych interesów wyłącznie w przypadku braku innej podstawy prawnej uzasadniającej przetwarzanie[17]. W przypadku przetwarzania

[14] „Opinia 06/2014 w sprawie pojęcia uzasadnionych interesów administratora danych zawartego w art. 7 dyrektywy 95/46/WE". Komisja Europejska, 9 kwietnia 2014 r. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf . Data uzyskania dostępu: 24 kwietnia 2017 r.

[15] Motywy 41 i 45 RODO.

[16] Grupa Robocza Art. 29, „Opinia 06/2014 w sprawie pojęcia uzasadnionych interesów administratora danych zawartego w art. 7 dyrektywy 95/46/WE", s. 19. Komisja Europejska, 9 kwietnia 2014 r. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf . Data uzyskania dostępu: 24 kwietnia 2017 r.

[17] Motyw 46 RODO.

szczególnej kategorii danych osobowych administrator byłby również zobowiązany do zapewnienia zgodności tego przetwarzania z wymogami art. 9 ust. 2 lit. c).

5. Art. 6 ust. 1 lit. e) – Niezbędność do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej

W niektórych przypadkach art. 6 ust. 1 lit. e) może stanowić odpowiednią podstawę uzasadniającą profilowanie w sektorze publicznym. W takim przypadku takie zadanie lub funkcja muszą mieć wyraźnie określoną podstawę prawną.

6. Art. 6 ust. 1 lit. f) – Niezbędność do celów wynikających z prawnie uzasadnionych interesów[18] realizowanych przez administratora lub stronę trzecią

Profilowanie uznaje się za dopuszczalne, jeżeli jest niezbędne do celów wynikających z prawnie uzasadnionych interesów[19] realizowanych przez administratora lub stronę trzecią. Przepisów art. 6 ust. 1 lit. f) nie stosuje się jednak automatycznie wyłącznie z uwagi na fakt, że administrator lub strona trzecia mają uzasadniony interes. Administrator musi przeprowadzić proces ważenia interesów, aby ocenić, czy interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, nie przeważają nad interesami administratora lub stron trzecich.

W tym kontekście za szczególnie istotne należy uznać następujące elementy:

- pozom szczegółowości profilu (sprofilowanie osoby, której dane dotyczą, w ramach szeroko określonej zbiorowości takiej jak „osoby interesujące się literaturą angielską" lub przypisanie jej do wąsko określonej kategorii pozwalającej traktować ją w spersonalizowany sposób);
- wszechstronność profilu (to, czy profil odnosi się wyłącznie do niewielkiej części aktywności osoby, której dane dotyczą, czy też stanowi pełniejszy obraz aktywności tej osoby);
- wpływ profilowania (skutki, jakie profilowanie wywiera na osobę, której dane dotyczą); oraz
- zabezpieczenia służące zapewnieniu rzetelności, niedyskryminującego charakteru i prawidłowości procesu profilowania.

Choć opinia Grupy Roboczej Art. 29 dotycząca uzasadnionych interesów[20] została wydana na podstawie art. 7 dyrektywy 95/46/WE o ochronie danych („dyrektywa"), zawarte w niej przykłady mogą być nadal przydatne i istotne dla administratorów zajmujących się profilowaniem. W opinii tej stwierdzono również, że administratorom byłoby trudno uzasadnić, że inwazyjne profilowanie i stosowanie praktyk pozwalających śledzić daną osobę w celach marketingowych lub reklamowych, na przykład praktyk polegających na śledzeniu aktywności danej osoby za pośrednictwem różnych stron internetowych, w różnych lokalizacjach, przy korzystaniu z różnych urządzeń i usług lub za pośrednictwem brokerów informacji, było zgodne z prawem z uwagi na ich uzasadniony interes.

[18] Uzasadnione interesy wymienione w motywie 47 RODO obejmują przetwarzanie do celów marketingu bezpośredniego i przetwarzanie bezwzględnie niezbędne do zapobiegania oszustwom.
[19] „Prawnie uzasadniony interes" administratora nie może skutkować uznaniem profilowania za zgodne z prawem, jeżeli dane przetwarzanie jest przetwarzaniem, o którym mowa w art. 22 ust. 1.
[20] Grupa Robocza Art. 29, „Opinia 06/2014 w sprawie pojęcia uzasadnionych interesów administratora danych zawartego w art. 7 dyrektywy 95/46/WE". Komisja Europejska, 9 kwietnia 2014 r., s. 47, przykłady na ss. 59 i 60 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf . Data uzyskania dostępu: 24 kwietnia 2017 r.

Oceniając zgodność przetwarzania z art. 6 ust. 1 lit. f), administrator powinien również wziąć pod uwagę kwestie związane z wykorzystywaniem lub łączeniem profili w przyszłości.

C. Art. 9 – Szczególne kategorie danych osobowych

Administratorzy mogą przetwarzać szczególne kategorie danych osobowych wyłącznie w przypadku, gdy są w stanie spełnić jeden z warunków określonych w art. 9 ust. 2, a także warunek ustanowiony w art. 6. Obejmuje to również dane należące do szczególnych kategorii, wywiedzione lub wywnioskowane z profilowania.

Profilowanie może doprowadzić do stworzenia danych szczególnej kategorii wskutek ich wywnioskowania z danych, które same w sobie nie są danymi szczególnej kategorii, ale które stają się nimi w momencie ich połączenia z innymi danymi. Przykładowo – na podstawie wykazu produktów spożywczych kupowanych przez daną osobę oraz informacji na temat jakości i wartości kalorycznej tych produktów można wywnioskować dane dotyczące stanu zdrowia tej osoby.

Jak wykazano na poniższym przykładzie, określone rodzaje informacji pozwalają odkryć korelacje umożliwiające wyciągnięcie pewnych wniosków co do stanu zdrowia, poglądów politycznych, przekonań religijnych lub orientacji seksualnej osób fizycznych:

Przykład

W ramach jednego z badań[21] „polubienia" na Facebooku zestawiono z ogólnymi informacjami ankietowymi na temat poszczególnych osób; opierając się na tych danych, badacze trafnie określili orientację seksualną użytkowników będących mężczyznami w 88% przypadków; ich pochodzenie etniczne w 95% przypadków; oraz to, czy są chrześcijanami czy muzułmanami w 82% przypadków.

Jeżeli na podstawie profilowania można wywnioskować wrażliwe informacje o preferencjach i cechach charakteru danej osoby, administrator powinien upewnić się, że:

- przetwarzanie nie jest niezgodne z pierwotnym celem, w jakim zbierano dane;
- wskazał podstawę wykazującą zgodność przetwarzania danych szczególnej kategorii z prawem; oraz
- udzielił osobie, której dane dotyczą, informacji o przetwarzaniu danych.

Zautomatyzowane podejmowanie decyzji, zdefiniowane w art. 22 ust. 1, w oparciu o szczególne kategorie danych osobowych stanowi przedmiot rozdziału IV (sekcja D).

D. Prawa osoby, której dane dotyczą[22]

[21] Michael Kosinski, David Stilwell i Thore Graepel. „Private traits and attributes are predictable from digital records of human behaviour" [„Cechy i przymioty charakteru można wywnioskować z cyfrowych zapisów informacji dotyczących zachowania osób"]. Badanie zlecone przez Narodową Akademię Nauk Stanów Zjednoczonych Ameryki, http://www.pnas.org/content/110/15/5802.full.pdf . Data uzyskania dostępu: 29 marca 2017 r.

[22] Sekcja ta ma zastosowanie zarówno do profilowania, jak i do zautomatyzowanego podejmowania decyzji. Należy pamiętać, że w odniesieniu do zautomatyzowanego podejmowania decyzji określonego w art. 22 zastosowanie mają również dodatkowe wymogi opisane w rozdziale IV.

RODO zwiększa prawa osób, których dane dotyczą, i nakłada nowe obowiązki na administratorów.

W kontekście profilowania prawa te są wykonywalne wobec administratora tworzącego dany profil i administratora odpowiedzialnego za zautomatyzowane podjęcie decyzji dotyczącej osoby, której dane dotyczą (niezależnie, czy miała miejsce interwencja ludzka), jeżeli nie jest to ten sam podmiot.

Przykład

Broker informacji przeprowadza proces profilowania danych osobowych. Zgodnie z obowiązkami przewidzianymi w art. 13 i 14 powinien on poinformować osobę fizyczną o przetwarzaniu jej danych, w tym musi stwierdzić, czy zamierza przekazać stworzony profil innym organizacjom. Broker informacji powinien również oddzielnie przedstawić informacje na temat prawa do sprzeciwu przewidzianego w art. 21 ust. 1.

Broker informacji przekazuje profil innemu przedsiębiorstwu. Na podstawie uzyskanego profilu przedsiębiorstwo to stosuje marketing bezpośredni wobec danej osoby fizycznej.

Przedsiębiorstwo to powinno poinformować daną osobę (art. 14 ust. 1 lit. c)), do jakich celów wykorzystuje ten profil i z jakiego źródła pochodzą dane (art. 14 ust. 2 lit. f)). Przedsiębiorstwo to musi ponadto poinformować osobę, której dane dotyczą, o jej prawie do sprzeciwu wobec przetwarzania, w tym profilowania, do celów marketingu bezpośredniego (art. 21 ust. 2).

Broker informacji i przedsiębiorstwo powinni zapewnić osobie, której dane dotyczą, możliwość korzystania z prawa dostępu do wykorzystanych danych (art. 15), prawa do sprostowania nieprawidłowych danych (art. 16) oraz w określonych okolicznościach prawa do usunięcia profilu lub danych osobowych wykorzystanych do jego utworzenia (art. 17). Osoba, której dane dotyczą, powinna również otrzymać informacje na temat jej profilu, na przykład informacje, do jakich „segmentów" lub „kategorii" została zakwalifikowana. [23]

Jeżeli przedsiębiorstwo wykorzystuje profil w ramach procesu podejmowania decyzji wyłącznie w sposób zautomatyzowany, a podjęta w ten sposób decyzja wywołuje skutki prawne wobec osoby, której dane dotyczą, lub w podobny sposób istotnie na nią wpływa, takie przedsiębiorstwo jest administratorem, do którego zastosowanie mają przepisy art. 22 (nie oznacza to wyłączenia brokera informacji z zakresu zastosowania art. 22, jeżeli przetwarzanie jest zgodne z odpowiednim progiem).

1. Art. 13 i 14 – Prawo do otrzymania informacji

Mając na uwadze, że podstawową zasadą leżącą u podstaw RODO jest zasada przejrzystości, administratorzy muszą w jasny i prosty sposób wyjaśnić osobom fizycznym, na czym polega profilowanie lub proces zautomatyzowanego podejmowania decyzji.

W szczególności, jeżeli przetwarzanie obejmuje podejmowanie decyzji na podstawie profilowania (niezależnie od tego, czy takie podejmowanie decyzji wchodzi w zakres stosowania przepisów

[23] Norweski organ ochrony danych. „The Great Data Race – How commercial utilisation of personal data challenges privacy" [„W pogoni za danymi – Zagrożenie dla prywatności, jakie niesie ze sobą wykorzystywanie danych osobowych do celów komercyjnych"], sprawozdanie, listopad 2015. https://www.datatilsynet.no/English/Publications/The-Great-Data-Race/. Data uzyskania dostępu: 24 kwietnia 2017 r.

art. 22), wówczas należy jasno poinformować osobę, której dane dotyczą, że jej dane są przetwarzane do celów zarówno a) profilowania, jak i b) podjęcia decyzji na podstawie uzyskanego profilu[24].

Motyw 60 stanowi, że udzielanie informacji na temat profilowania wchodzi w zakres obowiązków administratora dotyczących przejrzystości przewidzianych w art. 5 ust. 1 lit. a). Osoba, której dane dotyczą, ma prawo *do otrzymania informacji* od administratora o profilowaniu i w określonych okolicznościach prawo *do sprzeciwu* wobec profilowania *niezależnie* od tego, czy na podstawie profilowania są podejmowane w sposób całkowicie zautomatyzowany decyzje w indywidualnych przypadkach.

Dalsze wytyczne dotyczące przejrzystości w ujęciu ogólnym są dostępne w wytycznych Grupy Roboczej Art. 29 dotyczących przejrzystości na mocy RODO[25].

2. Art. 15 – Prawo dostępu

Art. 15 stanowi, że osoba, której dane dotyczą, jest uprawniona do uzyskania szczegółowych informacji dotyczących danych osobowych wykorzystanych do celów profilowania, w tym informacji, jakie kategorie danych zostały wykorzystane do stworzenia profilu.

Oprócz ogólnych informacji o przetwarzaniu danych zgodnie z art. 15 ust. 3 administrator ma obowiązek udostępnić dane wykorzystane do stworzenia profilu, a także musi umożliwić dostęp do informacji o profilu oraz o tym, do których segmentów została zakwalifikowana osoba, której dane dotyczą.

Prawo to różni się od prawa do przenoszenia danych przewidzianego w art. 20, w przypadku którego administrator nie musi przedstawiać samego profilu, a jedynie dane dostarczone przez osobę, której dane dotyczą, lub wynikające z obserwacji administratora[26].

W motywie 63 zapewniono pewien stopień ochrony administratorów obawiających się ujawnienia tajemnic handlowych lub naruszenia prawa własności intelektualnej, co może mieć szczególne znaczenie w kontekście profilowania. Motyw ten stanowi, że prawo dostępu „nie powinno negatywnie wpływać na prawa lub wolności innych osób, w tym tajemnice handlowe lub własność intelektualną, w szczególności na prawa autorskie chroniące oprogramowanie". Administratorzy nie mogą jednak uzasadniać odmowy udostępnienia lub przekazania informacji osobie, której dane dotyczą, powołując się na ochronę tajemnic handlowych.

Motyw 63 stanowi również, że „[w] miarę możliwości administrator powinien mieć możliwość udzielania zdalnego dostępu do bezpiecznego systemu, który zapewni osobie, której dane dotyczą, bezpośredni dostęp do jej danych osobowych".

[24] RODO – art. 13 ust. 1 lit. c) oraz art. 14 ust. 1 lit. c). Na podstawie art. 13 ust. 2 lit. f) i art. 14 ust. 2 lit. g) administrator musi poinformować osobę, której dane dotyczą, o stosowaniu zautomatyzowanego podejmowania decyzji, w tym profilowania, opisanych w art. 22 ust. 1 i 4. Więcej informacji na ten temat znajduje się w rozdziale IV.

[25] Grupa Robocza Art. 29, „Wytyczne dotyczące przejrzystości na mocy rozporządzenia 2016/679", WP260, 28 listopada 2017 r. http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850 . Data uzyskania dostępu: 18 grudnia 2017 r.

[26] Grupa Robocza Art. 29, „Wytyczne dotyczące prawa do przenoszenia danych", WP242, s. 9 http://ec.europa.eu/newsroom/document.cfm?doc_id=45685 . Data uzyskania dostępu: 8 stycznia 2018 r.

3. Art. 16 – Prawo do sprostowania danych, art. 17 – Prawo do usunięcia danych oraz art. 18 – Prawo do ograniczenia przetwarzania

Elementem profilowania może być prognozowanie, które zwiększa ryzyko nieprawidłowości. Dane wejściowe mogą być nieprawidłowe lub nieadekwatne, lub też mogą być wyrwane z kontekstu. Algorytm użyty do ustalenia korelacji może zawierać błędy.

Art. 16 dotyczący prawa do sprostowania danych może mieć zastosowanie na przykład w sytuacji, w której osoba fizyczna zostaje zakwalifikowania do kategorii, która określa jej zdolność do wykonania danego zadania, przy czym profil ten opiera się na nieprawidłowych informacjach. Osoby fizyczne mogą chcieć zakwestionować prawidłowość wykorzystanych danych oraz słuszność zakwalifikowania ich do danej grupy lub kategorii.

Prawa do sprostowania i usunięcia danych[27] dotyczą zarówno „wejściowych danych osobowych" (danych osobowych użytych do stworzenia profilu), jak i „danych wyjściowych" (samego profilu lub „punktacji" przyznanej danej osobie).

W art. 16 przewidziano również prawo osoby, której dane dotyczą, do uzupełnienia danych osobowych o dodatkowe informacje.

Przykład

System komputerowy wykorzystywany w lokalnej przychodni kwalifikuje daną osobę do grupy osób najbardziej narażonych na chorobę serca. Ten profil nie musi być nieprawidłowy, nawet jeżeli dana osoba nigdy nie cierpiała na chorobę serca.
Oznacza on jedynie, że w przypadku danej osoby *prawdopodobieństwo* zachorowania *jest większe*, co ze statystycznego punktu widzenia może znajdować odzwierciedlenie w rzeczywistości.

Biorąc pod uwagę cele przetwarzania, osoba, której dane dotyczą, ma jednak prawo do przedstawienia dodatkowego oświadczenia. W opisanej sytuacji takie dodatkowe oświadczenie mogłoby opierać się na przykład na bardziej zaawansowanym komputerowym systemie medycznym (i modelu statystycznym) uwzględniającym dodatkowe dane i przeprowadzającym bardziej szczegółowe oceny w porównaniu z wykorzystywanym w lokalnej przychodni systemem o bardziej ograniczonych możliwościach.

Prawo do ograniczenia przetwarzania (art. 18) ma zastosowanie na każdym etapie procesu profilowania.

4. Art. 21 – Prawo do sprzeciwu

Administrator musi *wyraźnie* poinformować osobę, której dane dotyczą, o prawie do sprzeciwu określonym w art. 21 ust. 1 i 2, a informacje na temat tego prawa musi przedstawić jasno i odrębnie od innych informacji (art. 21 ust. 4).

Na podstawie art. 21 ust. 1 osoba, której dane dotyczą, może wnieść sprzeciw wobec przetwarzania (w tym profilowania) z przyczyn związanych z jej szczególną sytuacją. Administratorzy są wyraźnie

[27] RODO – art. 17.[28] RODO – art. 18 ust. 1 lit. d).

zobowiązani do zapewnienia możliwości korzystania z tego prawa we wszystkich przypadkach, w których podstawą przetwarzania są przepisy art. 6 ust. 1 lit. e) lub f).

Jeżeli osoba, której dane dotyczą, skorzysta z tego prawa, wówczas administrator musi przerwać[28] proces profilowania (lub uniknąć jego rozpoczęcia), chyba że wykaże on istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą. Administrator może również być zobowiązany do usunięcia odpowiednich danych osobowych[29].

RODO nie zawiera żadnego wyjaśnienia, jakie podstawy zostałyby uznane za ważne i prawnie uzasadnione[30]. Przykładowo może zdarzyć się, że profilowanie jest korzystne dla ogółu społeczeństwa (lub szerszej społeczności), a nie jedynie z punktu widzenia interesów handlowych administratora, czego przykładem jest profilowanie do celów prognozowania rozprzestrzeniania się chorób zaraźliwych.

Administrator musiałby:

- rozważyć, na ile ważne jest stosowanie profilowania dla osiągnięcia danego celu;
- rozważyć wpływ profilowania na interesy, prawa i wolności osoby, której dane dotyczą, przy czym profilowanie powinno ograniczać się do minimum koniecznego do osiągnięcia danego celu; oraz
- przeprowadzić proces ważenia interesów.

We wszystkich przypadkach należy obowiązkowo przeprowadzić proces ważenia sprzecznych interesów – z jednej strony interesów administratora, a z drugiej względów (natury osobistej, społecznej lub zawodowej) będących podstawą wniesienia sprzeciwu przez osobę, której dane dotyczą. W przeciwieństwie do dyrektywy 95/46/WE ciężar dowodu na istnienie ważnych prawnie uzasadnionych podstaw spoczywa na administratorze, a nie na osobie, której dane dotyczą.

Z brzmienia art. 21 jasno wynika, że proces ważenia interesów w tym kontekście różni się od procesu określonego w art. 6 ust. 1 lit. f). Innymi słowy, wykazanie przez administratora, że jego wcześniejsza analiza uzasadnionego interesu była prawidłowa, jest niewystarczające. Proces ważenia interesów wymaga, aby uzasadniony interes był *ważny*, co implikuje konieczność osiągnięcia wyższego poziomu nadrzędności względem wnoszonych sprzeciwów.

W **art. 21 ust. 2** przewidziano *bezwarunkowe* prawo osoby, której dane dotyczą, do wniesienia sprzeciwu wobec przetwarzania dotyczących jej danych osobowych na potrzeby marketingu bezpośredniego, w tym profilowania, w zakresie, w jakim przetwarzanie jest związane z takim marketingiem bezpośrednim[31]. Oznacza to, że nie ma konieczności ważenia interesów, a administrator

[28] RODO – art. 18 ust. 1 lit. d).

[29] RODO – art. 17 ust. 1 lit. c).

[30] Wyjaśnienie pojęcia uzasadnionego interesu – zob. Grupa Robocza Art. 29, „Opinia 06/2014 w sprawie pojęcia uzasadnionych interesów administratora danych zawartego w art. 7 dyrektywy 95/46/WE" z dnia 9 kwietnia 2014 r., s. 24–26. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf . Data uzyskania dostępu: 24 kwietnia 2017 r.

[31] Zgodnie z art. 12 ust. 2 administrator, który zbiera od osób fizycznych dotyczące ich dane osobowe na potrzeby marketingu bezpośredniego, w momencie zbierania danych powinien rozważyć zapewnienie osobom, których dane dotyczą, łatwego sposobu na wskazanie, że nie życzą sobie, aby ich dane osobowe były wykorzystywane na potrzeby marketingu bezpośredniego, zamiast zmuszać je do skorzystania z przysługującego im prawa do sprzeciwu na późniejszym etapie.

musi zastosować się do woli danej osoby bez kwestionowania podstaw sprzeciwu. Dodatkowe informacje dotyczące tego prawa zawiera motyw 70, który stanowi, że wykonanie tego prawa jest możliwe w dowolnym momencie i jest bezpłatne.

IV. Przepisy szczególne dotyczące podejmowania decyzji wyłącznie w sposób zautomatyzowany zawarte w art. 22

Art. 22 ust. 1 stanowi, że:

> Osoba, której dane dotyczą, ma prawo do tego, by nie podlegać decyzji, która *opiera się wyłącznie* na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec tej osoby *skutki prawne* lub *w podobny sposób istotnie na nią wpływa*.

Użyty w tym przepisie termin „prawo" nie oznacza, że art. 22 ust. 1 ma zastosowanie dopiero wówczas, gdy osoba, której dane dotyczą, czynnie powołuje się na to prawo. W art. 22 ust. 1 ustanowiono ogólny zakaz podejmowania decyzji wyłącznie na podstawie zautomatyzowanego przetwarzania. Zakaz ten ma zastosowanie niezależnie od tego, czy osoba, której dane dotyczą, podejmuje działanie w związku z przetwarzaniem dotyczących jej danych osobowych.

Podsumowując, art. 22 stanowi, że:

(i) w pełni zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach, w tym profilowanie, wywołujące skutki prawne lub mające podobny istotny wpływ, jest ogólnie zabronione;
(ii) od zasady tej istnieją wyjątki;
(iii) w sytuacji zastosowania takich wyjątków muszą obowiązywać środki zabezpieczające prawa i wolności oraz uzasadnione interesy osoby, której dane dotyczą[32].

Taka wykładnia podkreśla ideę sprawowania kontroli przez osobę, której dane dotyczą, nad jej danymi osobowymi, co jest zgodne z zasadami leżącymi u podstaw RODO. Przyjęcie wykładni, zgodnie z którą art. 22 określa zakaz, a nie prawo, na które należy się powołać, oznacza, że osoby fizyczne są automatycznie objęte ochroną przed ewentualnymi skutkami tego rodzaju przetwarzania. Brzmienie tego artykułu sugeruje, że taki był jego zamysł, co znajduje potwierdzenie w motywie 71, który stanowi:

> Niemniej podejmowanie decyzji na podstawie takiego przetwarzania, w tym profilowania, **powinno być dozwolone**, w przypadku gdy jest to wyraźnie dopuszczone prawem Unii lub prawem państwa członkowskiego [...], lub gdy jest niezbędne do zawarcia lub wykonania umowy [...], lub gdy osoba, której dane dotyczą, wyraziła wyraźną zgodę.

Oznacza to, że przetwarzanie określone w art. 22 ust. 1 nie jest ogólnie dozwolone[33].

[32] Motyw 71 stanowi, że przetwarzanie takie powinno „podlegać odpowiednim zabezpieczeniom, obejmującym informowanie osoby, której dane dotyczą, prawo do uzyskania interwencji człowieka, prawo do wyrażenia własnego stanowiska, prawo do uzyskania wyjaśnienia co do decyzji wynikłej z takiej oceny oraz prawo do zakwestionowania takiej decyzji".

[33] Dalsze uwagi dotyczące wykładni art. 22 jako zakazu można znaleźć w załączniku 2.

Zakaz określony w art. 22 ust. 1 ma zastosowanie *wyłącznie* w szczególnych okolicznościach, w których decyzja podjęta wyłącznie w oparciu o zautomatyzowane przetwarzanie, w tym profilowanie, wywołuje wobec danej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa, jak wyjaśniono w dalszej części niniejszych wytycznych. Nawet w tych sytuacjach określono wyjątki umożliwiające stosowanie takiego przetwarzania.

Wymagane środki ochronne, które zostały bardziej szczegółowo omówione poniżej, obejmują określone w art. 13 i 14 prawo do otrzymania informacji (zwłaszcza istotnych informacji o zasadach podejmowania decyzji, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą) oraz zabezpieczenia, takie jak prawo do uzyskania interwencji ludzkiej oraz prawo do zakwestionowania tej decyzji (określone w art. 22 ust. 3).

Zawsze gdy przetwarzanie może powodować wysokie ryzyko wobec osoby, której dane dotyczą, administrator musi przeprowadzić ocenę skutków dla ochrony danych[34]. Ocena skutków dla ochrony danych nie tylko służy określaniu wszelkiego innego ryzyka związanego z przetwarzaniem, ale również może być szczególnie przydatna dla administratorów, którzy nie są pewni, czy proponowane przez nich działania spełnią definicję art. 22 ust. 1 oraz jakie środki ochronne muszą podjąć, jeśli dane działanie jest dozwolone na podstawie określonego wyjątku.

A. „Decyzja, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu"

W art. 22 ust. 1 jest mowa o decyzjach, „które opierają się wyłącznie" na zautomatyzowanym przetwarzaniu. Oznacza to brak interwencji ludzkiej w proces decyzyjny.

> **Przykład**
>
> Wynikiem zautomatyzowanego procesu jest w gruncie rzeczy zalecenie dotyczące osoby, której dane dotyczą. Jeżeli ostateczna decyzja zostaje podjęta przez człowieka po przeprowadzeniu oceny i uwzględnieniu innych czynników, taka decyzja nie „opiera się wyłącznie" na zautomatyzowanym przetwarzaniu.

Administrator nie może symulować interwencji ludzkiej, aby uniknąć sytuacji, w której zastosowanie ma art. 22. Przykładowo w przypadku rutynowego stosowania wobec osób fizycznych automatycznie generowanych profili bez jakiegokolwiek realnego wpływu na wynik nadal mamy do czynienia z decyzją, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu.

Aby działanie administratora mogło być uznane za interwencję ludzką, musi on zapewnić, aby nadzór nad podejmowaniem decyzji był istotny, a nie jedynie symboliczny. Takie działanie musi podejmować osoba, która ma uprawnienia i kompetencje do zmiany decyzji. Przeprowadzając analizę, taka osoba musi uwzględnić wszystkie istotne dane.

[34] Grupa Robocza Art. 29, „Wytyczne dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie »może powodować wysokie ryzyko« do celów rozporządzenia 2016/679", 4 kwietnia 2017 r. Komisja Europejska http://ec.europa.eu/newsroom/document.cfm?doc_id=44137 . Data uzyskania dostępu: 24 kwietnia 2017 r.

W ramach oceny skutków dla ochrony danych administrator powinien określić i udokumentować stopień interwencji ludzkiej w proces podejmowania decyzji oraz etap, na którym zachodzi taka interwencja ludzka.

B. „Skutki prawne" lub „podobny istotny wpływ"

W RODO uznaje się, że zautomatyzowane podejmowanie decyzji, w tym profilowanie, może mieć poważne skutki wobec osób fizycznych. Chociaż RODO nie zawiera definicji „skutków prawnych" lub „podobnego istotnego wpływu", to jednak brzmienie rozporządzenia wyraźnie wskazuje, że art. 22 obejmuje wyłącznie poważne skutki o znacznym wpływie.

„Decyzja wywołująca skutki prawne"

Jeżeli decyzja, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, wywołuje skutki prawne, oznacza to, że ma ona wpływ na prawa danej osoby przewidziane w przepisach, takie jak wolność do zrzeszania się, głosowania w wyborach lub wystąpienia na drogę sądową. Za skutek prawny można również uznać wpływ na status prawny danej osoby lub na prawa przysługujące jej na mocy umowy. Wśród przykładów takich skutków można wymienić decyzje dotyczące danej osoby fizycznej podjęte w sposób zautomatyzowany, które doprowadzają do:

- rozwiązania umowy;
- udzielenia lub odmowy udzielenia określonego świadczenia społecznego przewidzianego w obowiązujących przepisach, takiego jak świadczenie na dziecko lub dodatek mieszkaniowy;
- odmowy wjazdu na terytorium danego państwa lub odmowy nadania obywatelstwa.

„… w podobny sposób istotnie na nią wpływa"

Nawet w przypadku, gdy proces podejmowania decyzji nie wpływa na prawa poszczególnych osób, może wchodzić w zakres stosowania art. 22, jeżeli prowadzi do powstania skutku o równoważnym lub w podobny sposób istotnym wpływie.

Innymi słowy, nawet w przypadku, gdy nie doszło do zmiany praw ani obowiązków osoby, której dane dotyczą, proces podejmowania decyzji może wywrzeć na nią dostatecznie istotny wpływ, by osoba ta potrzebowała ochrony przewidzianej w tym przepisie. W RODO do zwrotu „istotny wpływ" dodano słowo „w podobny sposób" (które nie pojawiło się w art. 15 dyrektywy 95/46/WE). Dlatego też kryterium *istotnego wpływu* musi być zbliżone do kryterium, na podstawie którego uznaje się, że dana decyzja wywołuje skutek prawny.

W motywie 71 przedstawiono następujące typowe przykłady: „automatyczne odrzucenie elektronicznego wniosku kredytowego" lub „elektroniczne metody rekrutacji bez interwencji ludzkiej".

Aby można było uznać, że przetwarzanie danych wywiera istotny wpływ na określoną osobę, skutki tego przetwarzania muszą być dostatecznie znaczące lub istotne, by uzasadniały zainteresowanie się daną sprawą. Innymi słowy, decyzja musi stwarzać ryzyko:

- wywarcia istotnego wpływu na sytuację danej osoby, jej zachowanie lub podejmowane przez nią wybory;
- wywarcia długotrwałego lub trwałego wpływu na osobę, której dane dotyczą; lub
- w najbardziej ekstremalnym przypadku, doprowadzenia do wykluczenia lub dyskryminacji osób fizycznych.

Trudno jest precyzyjnie określić, jaki wpływ można by uznać za dostatecznie *istotny*, by spełniał to kryterium, choć do tej kategorii można byłoby zaliczyć następujące rodzaje decyzji:

- decyzje wywierające wpływ na sytuację finansową danej osoby, np. jej zdolność kredytową;
- decyzje wywierające wpływ na możliwość korzystania ze świadczeń zdrowotnych przez daną osobę;
- decyzje skutkujące utratą szansy na zatrudnienie przez daną osobę lub stawiające tę osobę w znacznie gorszej sytuacji;
- decyzje wywierające wpływ na dostęp danej osoby do kształcenia, na przykład na możliwość dostania się na studia.

Kwestie te są również powiązane ze zjawiskiem marketingu internetowego, który w coraz większym stopniu opiera się na zautomatyzowanych narzędziach i obejmuje całkowicie zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach. Niezależnie od konieczności zapewnienia zgodności z przepisami ogólnymi RODO opisanymi w rozdziale III, w poszczególnych przypadkach istotne mogą okazać się również przepisy proponowanego rozporządzenia w sprawie prywatności i łączności elektronicznej. Ponadto dodatkową ochroną muszą zostać objęte dzieci – kwestia te zostanie omówiona w rozdziale V poniżej.

W wielu typowych przypadkach decyzja o skierowaniu do danej osoby spersonalizowanej oferty reklamowej sporządzonej na podstawie rezultatów profilowania nie będzie wywierała podobnie istotnego wpływu na osoby fizyczne – na przykład reklama popularnego internetowego sklepu z odzieżą sporządzona w oparciu o prosty profil demograficzny: „kobiety z okolic Brukseli w wieku od 25 do 35 lat, które prawdopodobnie interesują się modą i określonego rodzaju artykułami odzieżowymi".

W niektórych sytuacjach takie decyzje mogą jednak wywrzeć tego rodzaju wpływ, w zależności od specyfiki danej sprawy, w tym:

- stopnia inwazyjności procesu profilowania, który może obejmować śledzenie aktywności osób fizycznych na różnych stronach internetowych oraz przy użyciu różnych urządzeń i usług;
- oczekiwań i woli zainteresowanych osób;
- sposobu dostarczenia materiału reklamowego; lub
- wykorzystywania wiedzy o czynnikach zwiększających podatność osób, których dane dotyczą.

Przetwarzanie danych, które może wywierać niewielki wpływ na ogół osób, może w istotny sposób wpływać na niektóre grupy społeczne takie jak mniejszości lub grupy osób dorosłych szczególnej troski. Na przykład osoba, co do której wiadomo, że boryka się z trudnościami finansowymi lub jest nimi zagrożona, i która jest regularnie adresatem reklam oferujących wysoko oprocentowane pożyczki, może skorzystać z tych ofert, potencjalnie zwiększając poziom swojego zadłużenia.

Zautomatyzowane podejmowanie decyzji, które prowadzi do zróżnicowania poziomu cen na podstawie danych osobowych lub cech charakteru, również może wywrzeć istotny wpływ na osoby, których dane dotyczą – na przykład ustanowienie zaporowo wysokich cen mogłoby uniemożliwić danej osobie uzyskanie dostępu do określonych towarów lub usług.

Podobnie istotny wpływ mogą również wywierać działania osób innych niż te, których dotyczy decyzja podjęta w zautomatyzowany sposób. Poniżej przedstawiono przykład takiej sytuacji.

Przykład

Operator kart kredytowych może teoretycznie obniżyć limit karty kredytowej danego klienta nie na podstawie jego własnej historii spłaty, ale w oparciu o nietradycyjne kryteria udzielania kredytów, takie jak analiza zachowań innych klientów żyjących na tym samym obszarze i robiących zakupy w tych samych sklepach.

Mogłoby to skutkować pozbawieniem niektórych osób możliwości z uwagi na działania podejmowane przez inne osoby.

W innym kontekście wykorzystywanie takich cech może przynieść korzyść w postaci udzielenia kredytu osobom, których wniosek kredytowy zostałby w innym przypadku odrzucony.

C. Wyjątki od zakazu

Jak opisano powyżej, w art. 22 ust. 1 ustanowiono ogólny zakaz podejmowania decyzji w indywidualnych przypadkach wyłącznie w sposób zautomatyzowany, jeżeli proces ten wywołuje skutki prawne wobec danej osoby lub w podobny sposób istotnie na nią wpływa.

Oznacza to, że administrator nie powinien przetwarzać danych w sposób opisany w art. 22 ust. 1, chyba że w danym przypadku zastosowanie ma jeden z wyjątków przewidzianych w art. 22 ust. 2 – tj. jeżeli dana decyzja jest:

a) niezbędna do wykonania lub zawarcia umowy;
b) dozwolona prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator i które przewiduje właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą; lub
c) opiera się na wyraźnej zgodzie osoby, której dane dotyczą.

Jeżeli proces podejmowania decyzji wiąże się z przetwarzaniem szczególnych kategorii danych osobowych zdefiniowanych w art. 9 ust. 1, administrator musi również upewnić się, że będzie w stanie zapewnić zgodność z wymogami ustanowionymi w art. 22 ust. 4.

1. Wykonanie umowy

Administratorzy mogą chcieć korzystać z całkowicie zautomatyzowanych procesów podejmowania decyzji, ponieważ mogą uznawać tę metodę za najodpowiedniejszą do osiągnięcia zamierzonego celu. Rutynowe przeprowadzanie interwencji ludzkiej może niekiedy okazać się niepraktyczne lub niemożliwe z uwagi na znaczną ilość przetwarzanych danych.

Administrator musi być w stanie wykazać, że zastosowanie tego rodzaju przetwarzania jest niezbędne, biorąc pod uwagę to, czy w danym przypadku możliwe jest zastosowanie metody, która w mniejszym stopniu ingerowałaby w prywatność [35]. Jeżeli w danym przypadku istnieją inne skuteczne sposoby osiągnięcia tego samego celu, których zastosowanie wiązałoby się z mniejszą ingerencją w prywatność, zastosowania tego rodzaju przetwarzania nie można byłoby uznać za „niezbędne".

[35] Buttarelli, Giovanni. „Assessing the necessity of measures that limit the fundamental right to the protection of personal data. A Toolkit" [„Ocena konieczności stosowania środków ograniczających prawo podstawowe do ochrony danych osobowych. Zestaw narzędzi"], Europejski Inspektor Ochrony Danych, 11 kwietnia 2017 r., https://edps.europa.eu/sites/edp/files/publication/17-04-11_necessity_toolkit_en_0.pdf Data uzyskania dostępu: 24 kwietnia 2017 r.

Zautomatyzowane podejmowanie decyzji, o którym mowa w art. 22 ust. 1, może okazać się również konieczne do celów związanych z przetwarzaniem danych przed zawarciem umowy.

Przykład

Przedsiębiorstwo publikuje ogłoszenie o wakacie. Z uwagi na duże zainteresowanie pracą dla tego przedsiębiorstwa na ogłoszenie odpowiadają dziesiątki tysięcy osób. Biorąc pod uwagę wyjątkowo dużą liczbę zgłoszeń, przedsiębiorstwo może uznać, że zidentyfikowanie odpowiednich kandydatów bez wcześniejszego przetworzenia danych w sposób zautomatyzowany, aby odsiać nieodpowiednie zgłoszenia, może okazać się niemożliwe ze względów praktycznych. W tej sytuacji zautomatyzowane podejmowanie decyzji może okazać się niezbędne do wyłonienia ograniczonej liczby potencjalnych kandydatów, z którymi przedsiębiorstwo mogłoby zawrzeć umowę.

W rozdziale III (sekcja B) przedstawiono dodatkowe informacje na temat umów rozumianych jako podstawa prawna uzasadniająca przetwarzanie.

2. Dopuszczenie prawem Unii lub prawem państwa członkowskiego

Zgodnie z art. 22 ust. 2 lit. b) zautomatyzowane podejmowanie decyzji, w tym profilowanie, może potencjalnie być dopuszczalne, jeżeli zostało dozwolone prawem Unii lub prawem państwa członkowskiego. W stosownych przepisach należy również ustanowić odpowiednie środki zapewniające osobie, której dane dotyczą, poszanowanie jej praw i wolności oraz prawnie uzasadnionych interesów.

Motyw 71 stanowi, że może wiązać się to z wykorzystywaniem zautomatyzowanego podejmowania decyzji, o którym mowa w art. 22 ust. 1, do monitorowania i zapobiegania oszustwom i uchylaniu się od podatków lub do zapewnienia bezpieczeństwa i niezawodności usług świadczonych przez administratora.

3. Wyraźna zgoda

W art. 22 ustanowiono wymóg uzyskania *wyraźnej* zgody. Przetwarzanie, które jest objęte zakresem definicji ustanowionej w art. 22 ust. 1, wiąże się z istotnym ryzykiem w zakresie ochrony danych, dlatego też w takim przypadku za odpowiednie rozwiązanie uznaje się zapewnienie wysokiego poziomu indywidualnej kontroli nad danymi osobowymi.

W RODO nie ustanowiono definicji „wyraźnej zgody". W wytycznych Grupy Roboczej Art. 29 dotyczących zgody[36] zawarto wskazówki dotyczące sposobu interpretowania tego pojęcia.

W rozdziale III (sekcja B) przedstawiono dodatkowe informacje dotyczące ogólnie zgody.

D. Szczególne kategorie danych osobowych – art. 22 ust. 4

[36] Grupa Robocza Art. 29, „Wytyczne dotyczące zgody na mocy rozporządzenia 2016/679", WP259. 28 listopada 2017 r., http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48849 . Data uzyskania dostępu: 18 grudnia 2017 r.

Zautomatyzowane podejmowanie decyzji (opisane w art. 22 ust. 1), w toku którego dochodzi do przetwarzania szczególnych kategorii danych osobowych, uznaje się za dopuszczalne wyłącznie w przypadku łącznego spełnienia następujących warunków (art. 22 ust. 4):

- możliwość zastosowania odstępstwa, o którym mowa w art. 22 ust. 2; oraz
- wystąpienie sytuacji, o której mowa w art. 9 ust. 2 lit. a) lub g).

Art. 9 ust. 2 lit. a) – wyraźna zgoda osoby, której dane dotyczą; lub

art. 9 ust. 2 lit. g) – przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.

W obydwu powyższych przypadkach administrator musi ustanowić odpowiednie środki zapewniające osobie, której dane dotyczą, poszanowanie jej praw i wolności oraz prawnie uzasadnionych interesów.

E. Prawa osoby, której dane dotyczą[37]

1. Art. 13 ust. 2 lit. f) i art. 14 ust. 2 lit. g) – Prawo do otrzymania informacji

Biorąc pod uwagę potencjalne ryzyko i skalę ingerencji, na jakie profilowanie w rozumieniu art. 22 naraża prawa osób, których dane dotyczą, administratorzy danych powinni szczególnie skrupulatnie wywiązywać się ze swoich zobowiązań w zakresie przejrzystości.

Zgodnie z art. 13 ust. 2 lit. f) i art. 14 ust. 2 lit. g) administratorzy są zobowiązani do podawania konkretnych, przystępnych informacji na temat zautomatyzowanego podejmowania decyzji odbywającego się wyłącznie na podstawie zautomatyzowanego przetwarzania, w tym profilowania, i wywołującego skutki prawne wobec danej osoby lub w podobny sposób istotnie na nią wpływającego[38].

Jeżeli administrator podejmuje zautomatyzowane decyzje w rozumieniu art. 22 ust. 1, musi:

- poinformować osobę, której dane dotyczą, o tym, że podejmuje takie decyzje;
- przekazać tej osobie istotne informacje o zasadach podejmowania tych decyzji; oraz
- udzielić tej osobie wyjaśnień w kwestii znaczenia i przewidywanych konsekwencji przetwarzania danych.

Udzielanie takich informacji ułatwi również administratorom wypełnienie wymogów w zakresie zabezpieczeń, o których mowa w art. 22 ust. 3 i motywie 71.

Udzielanie wskazanych powyżej informacji uznaje się za dobrą praktykę nawet w przypadku, gdy w danym przypadku zautomatyzowane podejmowanie decyzji i profilowanie nie odpowiada definicji ustanowionej w art. 22 ust. 1. W każdym razie administrator musi przekazać odpowiednie informacje

[37] W art. 12 RODO określono tryb wykonywania praw przez osobę, której dane dotyczą.

[38] W rozumieniu art. 22 ust. 1 i 4. W wytycznych Grupy Roboczej Art. 29 dotyczących przejrzystości omówiono ogólne wymogi udzielenia informacji ustanowione w art. 13 i 14.

osobie, której dane dotyczą, aby zagwarantować rzetelność przetwarzania[39] i spełnić wszystkie pozostałe wymogi udzielenia informacji przewidziane w art. 13 i 14.

Istotne informacje o „zasadach podejmowania decyzji"

Rozwój i złożoność zjawiska uczenia się maszyn może utrudniać zrozumienie sposobu działania zautomatyzowanego podejmowania decyzji lub profilowania.

Administrator powinien znaleźć prosty sposób na przedstawienie osobie, której dane dotyczą, uzasadnienia decyzji lub kryteriów, które doprowadziły do jej podjęcia. Zgodnie z przepisami RODO administrator jest zobowiązany do przekazania osobie, której dane dotyczą, istotnych informacji o zasadach podejmowania decyzji – informacje te niekoniecznie muszą mieć postać szczegółowego objaśnienia stosowanych algorytmów lub ujawnienia ich w całości[40]. Przekazywane informacje powinny jednak być na tyle wyczerpujące, by osoba, której dane dotyczą, zrozumiała powody podjętej decyzji.

Przykład

Administrator wykorzystuje wyniki punktowej oceny kredytowej, aby przeanalizować wniosek kredytowy złożony przez osobę fizyczną, i na tej podstawie odrzuca wniosek. Wspomniana ocena punktowa mogła zostać dostarczona przez biuro informacji kredytowej lub obliczona bezpośrednio na podstawie informacji, którymi dysponuje administrator.

Niezależnie od źródła, z którego pochodzi ta ocena (przy czym zgodnie z art. 14 ust. 2 lit. f) osobie, której dane dotyczą, należy udzielić informacji na temat źródła informacji, jeżeli dane osobowe nie zostały pozyskane od tej osoby), jeżeli administrator oparł się na wynikach oceny punktowej, musi objaśnić osobie, której dane dotyczą, wyniki tej oceny oraz zasady jej przeprowadzenia.

Administrator wyjaśnia, że proces ten ułatwia mu podejmowanie rzetelnych i odpowiedzialnych decyzji w kwestii udzielania kredytów. Administrator udziela osobie, której dane dotyczą, szczegółowych informacji na temat najważniejszych kwestii branych pod uwagę przy podejmowaniu decyzji, źródła tych informacji oraz ich znaczenia. Informacje te mogą obejmować na przykład:

- informacje podane przez osobę, której dane dotyczą, na formularzu wniosku;
- informacje na temat wcześniejszych zachowań tej osoby jako posiadacza rachunku, w tym informacje o wszelkich zaległościach w płatnościach; oraz
- informacje zaczerpnięte z urzędowych rejestrów publicznych, takie jak informacje z rejestru oszustw i z rejestrów upadłości.

Administrator informuje również osobę, której dane dotyczą, o tym, że stosowane metody przeprowadzania punktowej oceny kredytowej są regularnie testowane, aby zapewnić ich rzetelność, skuteczność i bezstronność.

[39] Motyw 60 RODO: „Administrator powinien podać osobie, której dane dotyczą, wszelkie inne informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania, uwzględniając konkretne okoliczności i konkretny kontekst przetwarzania danych osobowych. Ponadto należy poinformować osobę, której dane dotyczą, o fakcie profilowania oraz o konsekwencjach takiego profilowania".

[40] Złożoność problematyki nie zwalnia administratora z obowiązku przekazania stosownych informacji osobie, której dane dotyczą. Motyw 58 stanowi, że zasada przejrzystości „dotyczy [...] w szczególności sytuacji, gdy duża liczba podmiotów i złożoność technologiczna działań sprawiają, że osobie, której dane dotyczą, trudno jest dowiedzieć się i zrozumieć, czy dotyczące jej dane osobowe są zbierane, przez kogo oraz w jakim celu, na przykład w przypadku reklamy w internecie".

Administrator przekazuje osobie, której dane dotyczą, swoje dane kontaktowe, aby zapewnić jej możliwość wystąpienia o ponowne rozpatrzenie wydanej decyzji odmownej zgodnie z przepisami art. 22 ust. 3.

„Znaczenie" i „przewidywane konsekwencje"

Powyższe terminy oznaczają, że administrator jest zobowiązany do udzielania informacji na temat planowanego lub przyszłego przetwarzania i wpływu, jaki zautomatyzowane podejmowanie decyzji może wywrzeć na osobę, której dane dotyczą[41]. Aby przekazywane informacje były istotne i zrozumiałe, administrator powinien przedstawić autentyczne, konkretne przykłady takiego potencjalnego wpływu przetwarzania na osobę, której dane dotyczą.

W otoczeniu cyfrowym administratorzy mogą dysponować dodatkowymi narzędziami ułatwiającymi im przedstawienie tego rodzaju skutków.

Przykład

Zakład ubezpieczeń korzysta z procesu zautomatyzowanego podejmowania decyzji przy ustalaniu wysokości składek na ubezpieczenia komunikacyjne na podstawie wyników monitorowania stylu jazdy swoich klientów. Aby zilustrować znaczenie i przewidywane konsekwencje przetwarzania tego rodzaju danych, zakład ubezpieczeń wyjaśnia, że prowadzenie pojazdu w niebezpieczny sposób może skutkować ustaleniem wyższej kwoty składek ubezpieczeniowych, i udostępnia klientom aplikację porównującą fikcyjnych kierowców, z których jeden dopuszcza się niebezpiecznych zachowań na drodze, takich jak gwałtowne przyspieszanie i hamowanie w ostatnim możliwym momencie.

W aplikacji przedstawia się graficznie sposoby eliminowania niepożądanych zachowań, co pozwala na obniżenie wysokości składek ubezpieczeniowych.

Administratorzy mogą korzystać z podobnych technik wizualnej prezentacji danych, aby wyjaśnić, w jaki sposób podjęli określoną decyzję w przeszłości.

2. Art. 15 ust. 1 lit. h) – Prawo dostępu

Zgodnie z art. 15 ust. 1 lit. h) osoby, których dane dotyczą, są uprawnione do uzyskania tych samych informacji na temat podejmowania decyzji wyłącznie w sposób zautomatyzowany, w tym profilowania, co informacje przewidziane w wymogach ustanowionych w art. 13 ust. 2 lit. f) i art. 14 ust. 2 lit. g), mianowicie:

- informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu;
- istotne informacje o zasadach podejmowania decyzji; oraz
- wyjaśnienie znaczenia i przewidywanych konsekwencji takiego przetwarzania danych dla osoby, której dane dotyczą.

Administrator powinien był już przekazać osobie, której dane dotyczą, stosowne informacje w tym zakresie zgodnie z zobowiązaniami spoczywającymi na nim na mocy art. 13[42].

Art. 15 ust. 1 lit. h) stanowi, że administrator powinien przekazać osobie, której dane dotyczą, informacje na temat *przewidywanych konsekwencji* przetwarzania zamiast udzielać jej wyjaśnień dotyczących *konkretnej* decyzji. W motywie 63 przedstawiono wyjaśnienia w tym zakresie, stwierdzając, że każda osoba, której dane dotyczą, powinna mieć prawo do uzyskania „informacji" o zautomatyzowanym przetwarzaniu danych, w tym informacji o zasadach podejmowania decyzji w tym zakresie, a także – *przynajmniej* w przypadku decyzji podjętych na podstawie profilowania – o konsekwencjach takiego przetwarzania.

Wykonując swoje prawa wynikające z art. 15, osoba, której dane dotyczą, może dowiedzieć się o podjętej decyzji, która tej osoby dotyczy, w tym decyzji podjętej w oparciu o profilowanie.

Administrator powinien przedstawić osobie, której dane dotyczą, ogólne informacje (w szczególności informacje na temat czynników uwzględnionych w procesie podejmowania decyzji i na temat ich odpowiedniej wagi na poziomie zagregowanym), które mogą również służyć tej osobie do zakwestionowania tej decyzji.

F. Ustanawianie odpowiednich zabezpieczeń

Jeżeli podstawę przetwarzania stanowią art. 22 ust. 2 lit. a) lub c), zgodnie z art. 22 ust. 3 administratorzy są zobowiązani do wdrożenia właściwych środków ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą. Zgodnie z art. 22 ust. 2 lit. b) prawo Unii lub państwa członkowskiego zezwalające na przetwarzanie musi przewidywać również odpowiednie środki ochronne.

Powinny one obejmować co najmniej sposób, w jaki osoba, której dane dotyczą, może uzyskać interwencję ludzką, wyrazić własne stanowisko i zakwestionować decyzję.

Interwencja ludzka jest elementem kluczowym. Każdy przegląd musi podejmować osoba, która ma odpowiednie uprawnienia i zdolność do zmiany decyzji. Osoba przeprowadzająca przegląd powinna przeprowadzić dogłębną ocenę wszystkich właściwych danych, w tym wszelkich dodatkowych informacji przedstawionych przez osobę, której dane dotyczą.

W motywie 71 podkreślono, że odpowiednie zabezpieczenia powinny *zawsze* obejmować również:

udzielanie konkretnych informacji osobie, której dane dotyczą, i prawo [...] do uzyskania wyjaśnienia co do decyzji wynikłej z takiej oceny oraz prawo do zakwestionowania takiej decyzji.

Administrator musi zapewnić, by osoba, której dane dotyczą, mogła korzystać z tych praw w prosty sposób.

Stanowi to podkreślenie potrzeby, by przetwarzanie było przejrzyste. Osoba, której dane dotyczą, może zakwestionować decyzję lub przedstawić własne stanowisko tylko wówczas, gdy w pełni

[41] Rada Europy, „Draft Explanatory Report on the modernised version of CoE Convention 108" [„Projekt sprawozdania wyjaśniającego dotyczącego zmodernizowanej wersji Konwencji Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych"], pkt 75: „Osoby, których dane dotyczą, powinny mieć możliwość uzyskania informacji na temat podstaw merytorycznych przetwarzania ich danych oraz ich konsekwencji, a także na temat skutków takiego przetwarzania, w szczególności w przypadku wykorzystania algorytmów do celów automatycznego podejmowania decyzji, w tym do profilowania. Na przykład w przypadku punktowej oceny kredytowej osoby, których dane dotyczą, powinny mieć możliwość zapoznania się z zasadami, zgodnie z którymi przetwarzano ich dane i których zastosowanie doprowadziło do podjęcia pozytywnej lub negatywnej decyzji, a nie wyłącznie z informacjami na temat samej treści decyzji. Bez odpowiedniego zrozumienia tych kwestii skuteczne korzystanie z innych kluczowych zabezpieczeń takich jak prawo do sprzeciwu i prawo do wniesienia skargi do właściwego organu staje się niemożliwe". https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806b6ec2. Data uzyskania dostępu: 24 kwietnia 2017 r.

[42] W art. 12 ust. 3 RODO określono termin, w jakim należy przekazać te informacje.

rozumie, w jaki sposób i na jakiej podstawie podjęto decyzję. Wymogi dotyczące przejrzystości omówiono w rozdziale IV (sekcja E).

Błędy lub elementy stronniczości w zebranych lub udostępnionych danych bądź w zautomatyzowanym procesie podejmowania decyzji mogą skutkować:

- błędną klasyfikacją; oraz
- dokonaniem ocen na podstawie niedokładnych prognoz; które mają
- negatywny wpływ na osoby fizyczne.

Administratorzy powinni przeprowadzać częste oceny zbiorów danych, które przetwarzają, pod kątem występowania elementów stronniczości i opracować sposoby wyeliminowania elementów szkodliwych, w tym przypadków nadmiernego polegania na korelacjach.
Innymi przydatnymi środkami są systemy, w ramach których przeprowadza się audyty algorytmów, oraz regularne przeglądy prawidłowości i adekwatności zautomatyzowanego podejmowania decyzji, w tym profilowania.

Administratorzy powinni wprowadzić odpowiednie procedury i środki, aby zapobiegać błędom, nieprawidłowościom[43] lub dyskryminacji na podstawie danych należących do szczególnych kategorii. Środki te należy stosować cyklicznie; nie tylko na etapie projektowania, ale również w sposób ciągły, tak jak stosuje się profilowanie w odniesieniu do osób fizycznych. Rezultaty takiego badania należy następnie wykorzystać przy projektowaniu systemu.

Dalsze przykłady odpowiednich zabezpieczeń można znaleźć w sekcji Zalecenia.

V. Dzieci a profilowanie

W RODO nałożono na administratorów dodatkowe obowiązki dotyczące przetwarzania danych osobowych dzieci.

W samym art. 22 nie stosuje się rozróżnienia w zależności od tego, czy przetwarzanie danych dotyczy osób dorosłych, czy też dzieci. W motywie 71 stwierdzono jednak, że podejmowania decyzji wyłącznie w sposób zautomatyzowany, w tym profilowania, które wywołuje skutki prawne wobec danej osoby lub w podobny sposób istotnie na nią wpływa, nie należy stosować w odniesieniu do dzieci[44]. Z uwagi na fakt, że w samym artykule nie odzwierciedlono tego brzmienia, Grupa Robocza Art. 29 uważa, że sformułowanie to nie stanowi całkowitego zakazu przeprowadzania takiego rodzaju przetwarzania w odniesieniu do dzieci. W świetle tego motywu Grupa Robocza Art. 29 zaleca jednak, aby co do zasady administratorzy nie powoływali się na wyjątki przewidziane w art. 22 ust. 2, aby uzasadnić takie przetwarzanie.

Mogą jednak wystąpić pewne okoliczności, w których administratorzy muszą uciec się do w pełni zautomatyzowanego podejmowania decyzji, w tym do profilowania, które wywołuje wobec dzieci skutki prawne lub w podobny sposób istotnie na nie wpływa, na przykład aby chronić ich dobro.

[43] Motyw 71 RODO stanowi, że:
„Aby zapewnić rzetelność i przejrzystość przetwarzania wobec osoby, której dane dotyczą, mając na uwadze konkretne okoliczności i kontekst przetwarzania danych osobowych, administrator powinien stosować odpowiednie matematyczne lub statystyczne procedury profilowania, wdrożyć środki techniczne i organizacyjne zapewniające w szczególności korektę powodujących nieprawidłowości w danych osobowych i maksymalne zmniejszenie ryzyka błędów […]".

[44] Motyw 71 – „Takie przetwarzanie nie powinno dotyczyć dzieci".

Wówczas przetwarzanie można przeprowadzić na podstawie wyjątków przedstawionych w art. 22 ust. 2 lit. a), b) lub c), w zależności od sytuacji.

W takich przypadkach muszą obowiązywać odpowiednie zabezpieczenia zgodnie z wymogami art. 22 ust. 2 lit. b) i art. 22 ust. 3, a zabezpieczenia te muszą być odpowiednie dla dzieci. Administrator musi zapewnić, by zabezpieczenia te skutecznie chroniły prawa, wolności i uzasadnione interesy dzieci, których dane przetwarza.

Potrzebę szczególnej ochrony dzieci odzwierciedlono w motywie 38, który stanowi:

> Szczególnej ochrony danych osobowych wymagają dzieci, gdyż mogą one być mniej świadome ryzyka, konsekwencji, zabezpieczeń i praw przysługujących im w związku z przetwarzaniem danych osobowych. Taka szczególna ochrona powinna mieć zastosowanie przede wszystkim do wykorzystywania danych osobowych dzieci do celów *marketingowych lub do tworzenia profili osobowych lub profili użytkownika oraz do zbierania danych osobowych dotyczących dzieci, gdy korzystają one z usług skierowanych bezpośrednio do nich*.

W art. 22 nie zabroniono administratorom podejmowania decyzji dotyczących dzieci w sposób całkowicie zautomatyzowany, jeżeli decyzja nie wywołuje wobec dziecka skutków prawnych ani nie wpływa na nie w podobny istotny sposób. Niemniej jednak całkowicie zautomatyzowane podejmowanie decyzji, które mają wpływ na wybory i zachowanie dziecka, może potencjalnie wywoływać wobec dziecka skutki prawne lub podobnie istotne skutki, w zależności od charakteru danych wyborów i zachowań.

Z uwagi na fakt, że dzieci stanowią bardziej wrażliwą grupę społeczną, organizacje powinny co do zasady powstrzymać się od profilowania dzieci do celów marketingowych[45]. W środowisku internetowym dzieci mogą być szczególnie podatne oraz łatwiej ulegać wpływom reklamy behawioralnej. Na przykład w przypadku gier internetowych profilowanie można wykorzystać, by kierować oferty do graczy, którzy według algorytmu chętniej wydadzą pieniądze na grę, a także by wyświetlać bardziej spersonalizowane reklamy. Wiek i dojrzałość dziecka mogą wpływać na jego zdolność do zrozumienia powodów uzasadniających stosowanie tego rodzaju marketingu lub konsekwencje[46].

W art. 40 ust. 2 lit. g) wyraźnie odniesiono się do opracowywania kodeksów postępowania obejmujących zabezpieczenia dotyczące dzieci; istnieje również możliwość rozbudowywania istniejących kodeksów[47].

[45] W opinii Grupy Roboczej Art. 29 02/2013 w sprawie aplikacji na urządzenia inteligentne (WP202) przyjętej dnia 27 lutego 2013 r., na s. 26 sekcji 3.10 poświęconej konkretnie dzieciom, określono, że „administratorzy nie powinni przetwarzać danych dzieci na potrzeby reklamy behawioralnej, ani bezpośrednio, ani pośrednio, ponieważ będzie to przekraczać zdolności rozumienia dziecka i w związku z tym będzie wykraczać poza granice przetwarzania zgodnego z prawem".

[46] W badaniu UE na temat wpływu marketingu za pośrednictwem mediów społecznościowych, gier internetowych i aplikacji mobilnych na zachowanie dzieci stwierdzono, że praktyki marketingowe mają wyraźny wpływ na zachowanie dzieci. Badanie to przeprowadzono na dzieciach w wieku 6–12 lat.

[47] Przykładem kodeksu postępowania, w którym poruszono kwestię marketingu skierowanego na dzieci, jest kodeks postępowania opracowany przez Europejską Federację Marketingu Bezpośredniego (FEDMA) wraz z uzasadnieniem, dostępny pod adresem: http://www.oecd.org/sti/ieconomy/2091875.pdf . Data uzyskania dostępu: 15 maja 2017 r. Zob. w szczególności: „6.2 Sprzedawcy, którzy prowadzą działania ukierunkowane na dzieci lub których część grupy docelowej mogą stanowić dzieci, nie powinni nadużywać łatwowierności, lojalności, podatności lub braku doświadczenia dzieci"; „6.8.5 Sprzedawcy nie powinni uzależniać dostępu dziecka do strony internetowej od zebrania szczegółowych danych osobowych. W szczególności nie należy

VI. Ocena skutków dla ochrony danych i inspektor ochrony danych

Rozliczalność stanowi ważny aspekt i wyraźnie sformułowany wymóg RODO. [48]

Jako kluczowe narzędzie rozliczalności ocena skutków dla ochrony danych umożliwia administratorowi przeprowadzenie oceny ryzyka związanego z zautomatyzowanym podejmowaniem decyzji, w tym profilowaniem. Jest to sposób wykazania, że wdrożono odpowiednie środki mające na celu wyeliminowanie tych czynników ryzyka i udowodnienie zgodności z RODO.

W art. 35 ust. 3 lit. a) podkreślono potrzebę przeprowadzenia oceny skutków dla ochrony danych przez administratora w przypadku:

> *systematycznej, kompleksowej oceny* czynników osobowych odnoszących się do osób fizycznych, która *opiera się na* zautomatyzowanym przetwarzaniu, *w tym* profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną.

W art. 35 ust. 3 lit. a) odniesiono się do ocen, w tym profilowania i decyzji, które „opierają się" na zautomatyzowanym przetwarzaniu, a nie do decyzji, które opierają się „wyłącznie" na zautomatyzowanym przetwarzaniu. Przyjmujemy, że oznacza to, że art. 35 ust. 3 lit. a) będzie mieć zastosowanie w przypadku podejmowania decyzji, w tym profilowania, które wywołuje skutki prawne wobec danej osoby lub w podobny sposób istotnie na nią wpływa i które *nie* jest w pełni zautomatyzowane, a także do podejmowania decyzji w sposób całkowicie zautomatyzowany określonego w art. 22 ust. 1.

Jeżeli administrator przewiduje „model", w którym podejmuje decyzje wywierające *znaczny wpływ* na osoby fizyczne *wyłącznie* w sposób zautomatyzowany na podstawie stworzonych na temat tych osób *profili* i *nie może* polegać na zgodzie osób fizycznych, umowie zawartej z osobą fizyczną ani na przepisach prawa zezwalających na takie podejmowanie decyzji, administrator nie powinien realizować takich działań.

Administrator może nadal przewidywać „model" podejmowania decyzji w oparciu o profilowanie dzięki znacznemu zwiększeniu poziomu interwencji ludzkiej, aby model *przestał być w pełni zautomatyzowanym procesem podejmowania decyzji*, chociaż takie przetwarzanie może nadal stanowić ryzyko dla podstawowych praw i wolności osób fizycznych. W takim przypadku administrator musi zagwarantować wyeliminowanie tych czynników ryzyka i spełnienie wymogów opisanych w rozdziale III niniejszych wytycznych.

Ocena skutków dla ochrony danych może również pomóc administratorowi określić działania, które wprowadzi, aby wyeliminować ryzyko w zakresie ochrony danych związane z przetwarzaniem. Takie działania[49] mogłyby obejmować:

- informowanie osoby, której dane dotyczą, o stosowaniu zautomatyzowanego procesu podejmowania decyzji oraz o zasadach podejmowania decyzji;

stosować specjalnych zachęt, takich jak oferowanie nagród i gier, aby nakłonić dzieci do ujawnienia szczegółowych danych osobowych".

[48] Art. 5 ust. 2 RODO.

[49] Odzwierciedlenie wymogów określonych w art. 13 ust. 2 lit. f), art. 14 ust. 2 lit. g) i art. 22 ust. 3.

- wyjaśnienie znaczenia i przewidywanych konsekwencji przetwarzania danych dla osoby, której dane dotyczą;
- udostępnienie osobie, której dane dotyczą, środków sprzeciwu wobec decyzji; oraz
- umożliwienie osobie, której dane dotyczą, wyrażenia własnego stanowiska.

W zależności od cech szczególnych danego przypadku przeprowadzenie oceny skutków dla ochrony danych mogą uzasadniać inne działania związane z profilowaniem. Administratorzy mogą chcieć zapoznać się z wytycznymi Grupy Roboczej Art. 29 dotyczącymi oceny skutków dla ochrony danych[50], aby uzyskać dalsze informacje oraz pomoc w stwierdzeniu konieczności przeprowadzenia oceny skutków dla ochrony danych.

Dodatkowym wymogiem w zakresie rozliczalności jest wyznaczenie inspektora ochrony danych w przypadku, gdy profilowanie lub zautomatyzowane podejmowanie decyzji stanowi główną działalność administratora, która wymaga regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę (art. 37 ust. 1 lit. b))[51].

ZAŁĄCZNIK 1 – Zalecenia w zakresie dobrych praktyk

Następujące zalecenia w zakresie dobrych praktyk pomogą administratorom spełnić wymogi dotyczące profilowania i zautomatyzowanego podejmowania decyzji określone w przepisach RODO[52].

Artykuł	Kwestia	Zalecenie

[50] Grupa Robocza Art. 29, „Wytyczne dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie »może powodować wysokie ryzyko« do celów rozporządzenia 2016/679", 4 kwietnia 2017 r. http://ec.europa.eu/newsroom/document.cfm?doc_id=44137 . Data uzyskania dostępu: 24 kwietnia 2017 r.

[51] Grupa Robocza Art. 29, „Wytyczne dotyczące inspektorów ochrony danych (»DPO«)" 5 kwietnia 2017 r. http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048 . Data uzyskania dostępu: 22 stycznia 2018 r.

[52] Administratorzy muszą również zapewnić wdrożenie sprawnych procedur, aby zagwarantować wywiązanie się z obowiązków spoczywających na nich zgodnie z art. 15–22 w terminach przewidzianych w RODO.

Art. 5 ust. 1 lit. a) oraz art. 12, 13 i 14	Prawo do otrzymania informacji	Administratorzy powinni przeanalizować wytyczne Grupy Roboczej Art. 29 dotyczące przejrzystości (WP260) w celu zapoznania się z ogólnymi wymogami dotyczącymi przejrzystości. Poza spełnieniem ogólnych wymogów, w przypadku gdy administrator przetwarza dane zgodnie definicją w art. 22, musi on przedstawić istotne informacje o zasadach podejmowania decyzji. Zamiast przedstawiać złożone matematyczne wyjaśnienie dotyczące sposobu działania algorytmów lub uczenia się maszyn, administrator powinien rozważyć zastosowanie jasnych i wyczerpujących sposobów przekazania informacji osobie, której dane dotyczą, przedstawiając na przykład: • kategorie danych, które zostały lub zostaną wykorzystane do profilowania lub procesu podejmowania decyzji; • powody, dla których takie kategorie uznaje się za istotne; • sposób tworzenia poszczególnych profili wykorzystanych w zautomatyzowanym procesie podejmowania decyzji, w tym wszelkie statystyki wykorzystane w analizie; • powody, dla których dany profil jest istotny w zautomatyzowanym procesie podejmowania decyzji; oraz • sposób, w jaki zostanie on wykorzystany do podjęcia decyzji dotyczącej osoby, której dane dotyczą. Takie informacje będą na ogół miały większe znaczenie dla osoby, której dane dotyczą, i pomogą zwiększyć przejrzystość przetwarzania. Administratorzy mogą rozważyć zastosowanie wizualizacji i metod interaktywnych, aby zwiększyć przejrzystość działania algorytmów[53].
Art. 6 ust. 1 lit. a)	Zgoda jako podstawa uprawniająca do przetwarzania	Jeżeli administratorzy opierają się na zgodzie jako podstawie uprawniającej do przetwarzania danych, powinni zapoznać się z wytycznymi Grupy Roboczej Art. 29 dotyczącymi zgody (WP259).

[53] Information Commissioner's Office [Biuro Brytyjskiego Komisarza ds. Informacji], „Big data, artificial intelligence, machine learning and data protection version 2.0" [„Duże zbiory danych, sztuczna inteligencja, uczenie się maszyn a ochrona danych wersja 2.0"], marzec 2017 r., s. 87, pkt 194. https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf . Data uzyskania dostępu: 24 kwietnia 2017 r.

	danych	
Art. 15	Prawo dostępu	Administratorzy mogą zechcieć rozważyć wdrożenie mechanizmu umożliwiającego osobom, których dane dotyczą, sprawdzanie swojego profilu, tym szczegółów dotyczących informacji i źródeł wykorzystanych do jego opracowania.
Art. 16	Prawo do sprostowania danych	Administratorzy zapewniający osobom, których dane dotyczą, dostęp do ich profilu w związku z prawem tych osób określonym w art. 15 powinni umożliwić tym osobom aktualizację lub zmianę wszelkich nieprawidłowości dotyczących danych lub profilu. Może to również pomóc administratorom spełnić obowiązki określone w art. 5 ust. 1 lit. d). Administratorzy powinni rozważyć wprowadzenie internetowych narzędzi do zarządzania preferencjami, takich jak panel prywatności. Zapewnia to osobom, których dane dotyczą, możliwość zarządzania działaniami prowadzonymi w odniesieniu do ich danych w wielu różnych usługach – umożliwiając im zmianę ustawień, aktualizację danych osobowych i przegląd lub edycję profilu w celu poprawy ewentualnych nieprawidłowości.
Art. 21 ust. 1 i 2	Prawo do sprzeciwu	Osobę, której dane dotyczą, należy wyraźnie poinformować o przysługującym jej prawie do sprzeciwu, o którym mowa w art. 21 ust. 1 i 2, przedstawiając te informacje jasno i odrębnie od wszelkich innych informacji (art. 21 ust. 4). Administratorzy muszą zapewnić, by informację o tym prawie w widocznym miejscu na ich stronach internetowych lub w każdej innej istotnej dokumentacji oraz by nie została ona ukryta wśród innych warunków.
Art. 22 i motyw 71	Odpowiednie zabezpieczenia	Następująca lista, chociaż nie jest wyczerpująca, zawiera pewne sugestie w zakresie dobrych praktyk, które administratorzy mogą rozważyć podczas podejmowania decyzji wyłącznie w sposób zautomatyzowany, w tym profilowania (zgodnie z art. 22 ust. 1): • regularne kontrole jakości systemów w celu zagwarantowania, że osoby fizyczne traktowane są sprawiedliwie i nie są dyskryminowane, czy to na podstawie przypisania do szczególnych kategorii danych osobowych, czy też z innego powodu; • audyty z wykorzystaniem algorytmów – badanie algorytmów wykorzystanych i opracowanych przez systemy uczenia się maszyn w celu udowodnienia, że rzeczywiście działają zgodnie z przeznaczeniem i nie prowadzą do uzyskana dyskryminujących, błędnych lub nieuzasadnionych wyników; • w odniesieniu do audytów przeprowadzanych przez niezależną „stronę trzecią" (jeżeli podejmowanie decyzji opierające się na profilowaniu ma znaczny wpływ na osoby fizyczne) – zapewnienie audytorowi wszelkich niezbędnych informacji na temat działania algorytmów lub systemów uczenia się maszyn; • uzyskanie w odniesieniu do algorytmów strony trzeciej zapewnienia umownego o przeprowadzeniu audytu

		i badania oraz o tym, ze algorytmy są zgodne z ustalonymi normami; • szczególne środki dotyczące minimalizacji danych w celu wprowadzenia jasnych okresów przechowywania profili i wszelkich danych osobowych wykorzystanych do tworzenia lub stosowania profili; • stosowanie technik anonimizacji lub pseudonimizacji w kontekście profilowania; • umożliwienie osobie, której dane dotyczą, wyrażenia własnego stanowiska i zakwestionowania decyzji; oraz • mechanizm interwencji ludzkiej w określonych przypadkach, na przykład zapewnienie odnośnika do procesu odwołania w chwili przedstawiania zautomatyzowanej decyzji osobie, której dane dotyczą, z ustalonymi terminami dotyczącymi przeglądu i określonym punktem kontaktowym do przesyłania ewentualnych pytań. Administratorzy mogą również rozważyć następujące możliwości: • mechanizm certyfikacji operacji przetwarzania; • kodeksy postępowania dotyczące procedur audytu uwzględniających uczenie się maszyn; • rady oceny etycznej oceniające potencjalne szkody i korzyści dla społeczeństwa wynikające z rozmaitych zastosowań profilowania.

ZAŁĄCZNIK 2 – Kluczowe przepisy RODO

Kluczowe przepisy RODO odnoszące się do profilowania do celów ogólnych i zautomatyzowanego podejmowania decyzji

Artykuł	Motyw	Uwagi
Art. 3 ust. 2 lit. b)	**24**	Monitorowanie zachowania osób, których dane dotyczą, o ile do zachowania tego dochodzi w Unii. **Motyw 24** „[osoby fizyczne są] obserwowane w internecie [...] stosowane są techniki przetwarzania danych polegające na profilowaniu osoby fizycznej, *w szczególności w celu podjęcia decyzji* jej dotyczącej lub przeanalizowania lub prognozowania jej osobistych preferencji, zachowań i postaw".
Art. 4 pkt 4	**30**	Definicja profilowania zawarta w **art. 4 pkt 4**. **Motyw 30** „Osobom fizycznym mogą zostać przypisane identyfikatory internetowe – takie

		jak adresy IP, identyfikatory plików cookie, [...] czy też inne identyfikatory, generowane na przykład przez etykiety RFID [...] Może to skutkować zostawianiem śladów, które w szczególności w połączeniu z unikatowymi identyfikatorami i innymi informacjami uzyskiwanymi przez serwery *mogą być wykorzystywane do tworzenia profili i do identyfikowania tych osób*".
Art. 5 i 6	**72**	**Motyw 72**: „Profilowanie podlega przepisom niniejszego rozporządzenia dotyczącym przetwarzania danych osobowych, takim jak przepisy określające podstawy prawne przetwarzania **(art. 6)** lub zasady ochrony danych **(art. 5)**".
Art. 8	**38**	Wykorzystanie danych osobowych dzieci do celów profilowania. **Motyw 38:** „Szczególnej ochrony [...] wymagają dzieci [...] [ochrona] powinna mieć zastosowanie przede wszystkim do wykorzystywania danych osobowych dzieci do celów [...] tworzenia profili osobowych lub profili użytkownika [...]".
Art. 13 i 14	**60**	Prawo do otrzymania informacji. **Motyw 60**: „Ponadto *należy poinformować osobę, której dane dotyczą, o fakcie profilowania oraz o konsekwencjach takiego profilowania*".
Art. 15	**63**	Prawo dostępu. **Motyw 63:** „[...] prawo do wiedzy i informacji [...] w zakresie celów, w jakich dane osobowe są przetwarzane [...] oraz, *przynajmniej* w przypadku profilowania, konsekwencji takiego przetwarzania".
Art. 21 ust. 1, 2 i 3	**70**	Prawo do sprzeciwu wobec profilowania. **Motyw 70** „[...] powinna mieć prawo wnieść [...] sprzeciw wobec tego przetwarzania [...] w tym profilowania, o ile jest ono powiązane z marketingiem bezpośrednim".
Art. 23	**73**	**Motyw 73:** „W prawie Unii lub w prawie państwa członkowskiego można przewidzieć ograniczenia dotyczące określonych zasad oraz [...] prawa do sprzeciwu, decyzji opartych na profilowaniu [...] o ile jest to niezbędne i proporcjonalne w społeczeństwie demokratycznym, [...]" by zapewnić ochronę szczególnych celów leżących w ogólnym interesie publicznym.
Art. 35 ust. 3 lit. a)	**91**	Wymaga się przeprowadzenia oceny skutków dla ochrony danych w przypadku „systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która *opiera się* na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną;". **Obejmuje podejmowanie decyzji, w tym profilowanie, które nie opiera się wyłącznie na zautomatyzowanym przetwarzaniu**.

Kluczowe przepisy RODO odnoszące się do zautomatyzowanego podejmowania decyzji w rozumieniu art. 22

Artykul	Motyw	Uwagi
Art. 13 ust. 2 lit. f)	**61**	Prawo do uzyskania: • informacji na temat stosowania zautomatyzowanego podejmowania decyzji na podstawie **art. 22 ust. 1** i **4**;

oraz **art. 14 ust. 2 lit. g)**		• istotnych informacji o zasadach podejmowania decyzji; • informacji o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania danych.
Art. 15 ust. 1 lit. h)		Szczególne prawa dostępu do informacji na temat podejmowania decyzji wyłącznie w sposób zautomatyzowany, w tym profilowania.
Art. 22 ust. 1	**71**	Zakaz podejmowania decyzji, które wywołują skutki prawne lub mają podobny istotny wpływ, w oparciu wyłącznie o zautomatyzowane przetwarzanie, w tym profilowanie. Poza wyjaśnieniem przedstawionym w tekście głównym wytycznych, poniżej rozwinięto uzasadnienie interpretowania art. 22 jako zakazu: • Chociaż rozdział III dotyczy praw osoby, której dane dotyczą, przepisy art. 12–22 nie odnoszą się wyłącznie do *czynnego* wykonywania praw. Niektóre prawa są *bierne*; nie wszystkie odnoszą się do sytuacji, gdy osoba, której dane dotyczą, podejmuje działanie, tj. składa wniosek lub skargę lub pewnego rodzaju żądanie. Art. 15–18 i art. 20–21 odnoszą się do czynnego wykonywania praw przez osobę, której dane dotyczą, ale art. 13 i 14 dotyczą obowiązków, które musi spełnić administrator danych bez czynnego zaangażowania osoby, której dane dotyczą. W związku z tym włączenie art. 22 do tego rozdziału samo w sobie nie oznacza prawa do sprzeciwu. • W art. 12 ust. 2 jest mowa o wykonywaniu przez osobę, której dane dotyczą, praw przysługujących jej na mocy art. 15–22. Nie oznacza to jednak, że sam art. 22 ust. 1 należy interpretować jako prawo. Na mocy art. 22 osobie, której dane dotyczą, *przysługuje* czynne prawo, ale stanowi ono część zabezpieczeń, które należy stosować w przypadkach, gdy dozwolone jest zautomatyzowane podejmowanie decyzji (art. 22 ust. 2 lit. a)–c)) – prawo do uzyskania interwencji ludzkiej, do wyrażenia własnego stanowiska i do zakwestionowania decyzji. Artykuł ten ma zastosowanie tylko w tych przypadkach, ponieważ przeprowadzenie przetwarzania opisanego w art. 22 ust. 1 na innej podstawie jest zakazane. • Art. 22 umieszczono w sekcji RODO zatytułowanej „Prawo do sprzeciwu **oraz** zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach", co oznacza, że na mocy art. 22 *nie* nadano prawa do sprzeciwu, jak ma to miejsce w przypadku art. 21. Podkreśla to również nieuwzględnienie w art. 22 wyraźnego obowiązku informacyjnego równoważnego obowiązkowi zawartemu w art. 21 ust. 4. • Gdyby art. 22 należało interpretować jako prawo do sprzeciwu, wyjątek zawarty w art. 22 ust. 2 lit. c) byłby pozbawiony sensu. Wyjątek stanowi, że zautomatyzowane podejmowanie decyzji można nadal przeprowadzić po otrzymaniu wyraźnej zgody osoby, której dane dotyczą (zob. poniżej). Stanowiłoby to sprzeczność, ponieważ osoba, której dane dotyczą, nie może sprzeciwiać się i wyrażać zgody na to samo przetwarzanie. • Sprzeciw oznaczałby, że musi nastąpić interwencja ludzka. Wyjątki określone w art. 22 ust. 2 lit. a) i c) są nadrzędne względem głównej zasady przedstawionej w art. 22 ust. 1, lecz jedynie wówczas, gdy

		osoba, której dane dotyczą, może uzyskać interwencję ludzką, jak określono w art. 22 ust. 3. Z uwagi na fakt, że (wyrażając sprzeciw) osoba, której dane dotyczą, zażądała już interwencji ludzkiej, w każdym przypadku następuje automatyczne obejście art. 22 ust. 2 a) i c), co sprawia, że artykuły te są bezprzedmiotowe. **Motyw 71**: „Do takiego przetwarzania zalicza się »profilowanie« – które polega na dowolnym zautomatyzowanym przetwarzaniu danych osobowych pozwalającym ocenić czynniki osobowe osoby fizycznej, a w szczególności analizować lub prognozować aspekty dotyczące efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się osoby, której dane dotyczą [...]". „*Takie przetwarzanie nie powinno dotyczyć dzieci*".
Art. 22 ust. 2 lit. a)–c)	**71**	**W art. 22 ust. 2** zwalnia się z zakazu przetwarzania w sytuacjach **a)** wykonania lub zawarcia umowy, **b)** dopuszczenia prawem Unii lub prawem państwa członkowskiego lub **c)** wyraźnej zgody. **W motywie 71** przedstawiono szerszy kontekst dotyczący **art. 22 ust. 2 lit. b)** i stwierdzono, że przetwarzanie opisane w **art. 22 ust. 1**: „[...] powinno być dozwolone, w przypadku gdy jest to wyraźnie dopuszczone prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator, w tym do celów monitorowania i zapobiegania – zgodnie z uregulowaniami, standardami i zaleceniami instytucji Unii lub krajowych podmiotów nadzorujących – oszustwom i uchylaniu się od podatków oraz do zapewniania bezpieczeństwa i niezawodności usług świadczonych przez administratora [...]".
Art. 22 ust. 3	**71**	**W art. 22 ust. 3 i w motywie 71** określono również, że nawet w przypadkach, o których mowa w **art. 22 ust. 2 lit. a)** i **c)**, przetwarzanie takie powinno podlegać odpowiednim zabezpieczeniom. **Motyw 71:** „[...] obejmującym informowanie osoby, której dane dotyczą, prawo do uzyskania interwencji człowieka, prawo do wyrażenia własnego stanowiska, prawo do uzyskania wyjaśnienia co do decyzji wynikłej z takiej oceny oraz prawo do zakwestionowania takiej decyzji. Takie przetwarzanie nie powinno dotyczyć dzieci".
Art. 23	**73**	**Motyw 73:** „W prawie Unii lub w prawie państwa członkowskiego można przewidzieć ograniczenia dotyczące określonych zasad oraz [...] prawa do sprzeciwu, decyzji opartych na profilowaniu [...] o ile jest to niezbędne i proporcjonalne w społeczeństwie demokratycznym, [...]" by zapewnić ochronę szczególnych celów leżących w ogólnym interesie publicznym.
Art. 35 ust. 3 lit. a)	**91**	Wymóg przeprowadzenia oceny skutków dla ochrony danych.
Art. 47 ust. 2 lit. e)		Wiążące reguły korporacyjne, o których mowa w **art. 47 ust. 1**, powinny zawierać co najmniej określenie „[...] prawa do niepodlegania decyzjom opartym wyłącznie na zautomatyzowanym przetwarzaniu – w tym profilowaniu – zgodnie z **art. 22** [...]".

ZAŁĄCZNIK 3 – Materiały uzupełniające

W niniejszych wytycznych uwzględniono następujące dokumenty:

- Grupa Robocza Art. 29, „Porady dotyczące najważniejszych elementów definicji i przepisów w zakresie profilowania w ramach ogólnego rozporządzenia UE o ochronie danych UE", dokument przyjęty dnia 13 maja 2013 r.;
- Grupa Robocza Art. 29, „Opinia 2/2010 w sprawie internetowej reklamy behawioralnej", WP 171;
- Grupa Robocza Art. 29, „Opinia 03/2013 w sprawie ograniczenia celu", WP 203;
- Grupa Robocza Art. 29, „Opinia 06/2014 w sprawie pojęcia uzasadnionych interesów administratora danych zawartego w art. 7 dyrektywy 95/46/WE", WP 217
- Grupa Robocza Art. 29, „Oświadczenie dotyczące roli opartego na analizie ryzyka podejścia do ram prawnych w zakresie ochrony danych", WP 218;
- Grupa Robocza Art. 29, „Opinia 8/2014 w sprawie najnowszych osiągnięć w zakresie internetu rzeczy", WP 223;
- Grupa Robocza Art. 29, „Wytyczne dotyczące inspektorów ochrony danych (»DPO«)", WP 243;
- Grupa Robocza Art. 29, „Wytyczne dotyczące ustalania wiodącego organu nadzorczego właściwego dla administratora lub podmiotu przetwarzającego", WP 244;
- Grupa Robocza Art. 29, „Wytyczne dotyczące zgody", WP 259
- Grupa Robocza Art. 29, „Wytyczne dotyczące przejrzystości", WP 260
- Rada Europy, „Recommendation CM/Rec(2010)13 on the protection of individuals with regard to automatic processing of personal data in the context of profiling" [„Zalecenie CM/Rec(2010)13 w sprawie ochrony osób fizycznych w związku z automatycznym przetwarzaniem danych osobowych w kontekście tworzenia profili"];
- Rada Europy, „Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data" [„Wytyczne dotyczące ochrony osób fizycznych w związku z przetwarzaniem danych osobowych w świecie dużych zbiorów danych"], styczeń 2017 r.
- Biuro Brytyjskiego Komisarza ds. Informacji, „Big data, artificial intelligence, machine learning and data protection version 2.0" [„Duże zbiory danych, sztuczna inteligencja, uczenie się maszyn i ochrona danych wersja 2.0"], marzec 2017 r.
- Biuro Australijskiego Komisarza ds. Informacji, „Consultation draft: Guide to big data and the Australian Privacy Principles" [„Projekt do konsultacji: Wytyczne w sprawie dużego zbioru danych w kontekście australijskich zasady ochrony prywatności"] z maja 2016 r.
- Europejski Inspektor Ochrony Danych, „Opinia 7/2015 – Stawianie czoła wyzwaniom związanym z dużymi zbiorami danych", 19 listopada 2015 r.
- Datatilsynet, „Big Data – privacy principles under pressure" [„Duże zbiory danych - przepisy dotyczące prywatności pod szczególną presją"], wrzesień 2013 r.
- Rada Europy, Konwencja o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, „Draft explanatory report on the modernised version of CoE Convention 108" [„Projekt sprawozdania wyjaśniającego w sprawie zaktualizowanej wersji konwencji nr 108 RE"], sierpień 2016 r.
- Datatilsynet, „The Great Data Race – How commercial utilisation of personal data challenges privacy. Report" [„W pogoni za danymi – Zagrożenie dla prywatności, jakie niesie ze sobą wykorzystywanie danych osobowych do celów komercyjnych"], listopad 2015 r.
- Europejski Inspektor Ochrony Danych, „Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit" [„Ocenia konieczności

wprowadzenia środków ograniczających prawo podstawowe do ochrony danych osobowych: Zestaw narzędzi"]

- Wspólny Komitet Europejskich Urzędów Nadzoru, „Joint Committee Discussion Paper on the use of Big Data by financial institutions 2016-86" [„Dokument Wspólnego Komitetu 2016-86 otwierający debatę na temat wykorzystywania dużych zbiorów danych przez instytucje finansowe"]. https://www.esma.europa.eu/sites/default/files/library/jc-2016-86_discussion_paper_big_data.pdf
- Commission de la protection de la vie privée [Belgijska Komisja Ochrony Prywatności], „Big Data Rapport" https://www.privacycommission.be/sites/privacycommission/files/documents/Big%20Data%20voor%20MindMap%2022-02-17%20fr.pdf
- Senat Stanów Zjednoczonych, Komisja ds. Handlu, Nauki i Transportu. „A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes, Staff Report for Chairman Rockefeller" [„Przegląd działalności brokerów informacji: gromadzenie, wykorzystywanie i sprzedaż danych konsumentów do celów marketingowych – sprawozdanie służb dla przewodniczącego Rockefellera"], 18 grudnia 2013 r. https://www.commerce.senate.gov/public/_cache/files/0d2b3642-6221-4888-a631-08f2f255b577/AE5D72CBE7F44F5BFC846BECE22C875B.12.18.13-senate-commerce-committee-report-on-data-broker-industry.pdf
- L. Edwards i M. Veale, „Slave to the Algorithm? Why a »Right to an Explanation« is probably not the remedy you are looking for" [„Niewolnik algorytmu? Dlaczego »prawo do zażądania wyjaśnień« prawdopodobnie nie jest najlepszym rozwiązaniem"], opracowanie opublikowane dnia 24 maja 2017 r. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2972855
- NYTimes.com, „Showing the Algorithms behind New York City Services" [„Przedstawienie algorytmów stosowanych na potrzeby usług w Nowym Jorku"] https://mobile.nytimes.com/2017/08/24/nyregion/showing-the-algorithms-behind-new-york-city-services.html?referer=https://t.co/6uUVVjOIXx?amp=1 . Data uzyskania dostępu: 24 sierpnia 2017 r.
- Rada Europy, „Recommendation CM/REC(2018)x of the Committee of Ministers to Member States on Guidelines to promote, protect and fulfil children's rights in the digital environment" [„Zalecenie Komitetu Ministrów CM/REC(2018)x do państw członkowskich w sprawie wytycznych dotyczących promowania, ochrony i realizacji praw dzieci w otoczeniu cyfrowym"], (zmieniony projekt z dnia 25 lipca 2017 r.). https://www.coe.int/en/web/children/-/call-for-consultation-guidelines-for-member-states-to-promote-protect-and-fulfil-children-s-rights-in-the-digital-environment?inheritRedirect=true&redirect=%2Fen%2Fweb%2Fchildren Data uzyskania dostępu: 31 sierpnia 2017 r.
- Unicef, „Privacy, protection of personal information and reputation rights, Discussion paper series: Children's Rights and Business in a Digital World" [„Prawa do ochrony prywatności, danych osobowych i reputacji, seria dokumentów konsultacyjnych: Prawa i sprawy dzieci w świecie cyfrowym"]. https://www.unicef.org/csr/files/UNICEF_CRB_Digital_World_Series_PRIVACY.pdf Data uzyskania dostępu: 31 sierpnia 2017 r.
- Izba Lordów, „Growing up with the internet. Select Committee on Communications, 2nd Report of Sessions 2016–17" [„Dorastanie z dostępem do internetu. Komitet Specjalny ds. Komunikacji, drugie sprawozdanie z sesji z lat 2016–2017"]. https://publications.parliament.uk/pa/ld201617/ldselect/ldcomuni/130/13002.htm Data uzyskania dostępu: 31 sierpnia 2017 r.
- S. Wachter, B. Mittelstadt i L. Floridi, „Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation" [„Dlaczego ogólne rozporządzenie o ochronie danych nie obejmuje prawa do zażądania wyjaśnień w kwestii zautomatyzowanego podejmowania decyzji?"]. 28 grudnia 2016 r. https://www.turing.ac.uk/research_projects/data-ethics-group-deg/. Data uzyskania dostępu: 13 grudnia 2017 r.

- S. Wachter, B. Mittelstadt i C. Russell, „Counterfactual explanations Without Opening the Black Box: Automated Decisions and the GDPR" [„Alternatywne wyjaśnienia niewymagające otwarcia »czarnej skrzynki«: decyzje zautomatyzowane a RODO"], 6 października 2017 r. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3063289 Data uzyskania dostępu: 13 grudnia 2017 r.
- Rząd Australii, „Better Practice Guide, Automated Assistance in Administrative Decision-Making. Six steps methodology, plus summary of checklist points Part 7" [„Przewodnik lepszych praktyk, Zautomatyzowana pomoc w podejmowaniu decyzji administracyjnych. Metoda sześciu kroków oraz część 7 »Podsumowanie list kontrolnych«"], luty 2007 r. https://www.oaic.gov.au/images/documents/migrated/migrated/betterpracticeguide.pdf Data uzyskania dostepu: 9 stycznia 2018 r.

GRUPA ROBOCZA ART. 29

18/PL

WP250rev.01

Wytyczne dotyczące zgłaszania naruszeń ochrony danych osobowych zgodnie z rozporządzeniem 2016/679

Przyjęte w dniu 3 października 2017 r.

Ostatnio zmienione i przyjęte w dniu 6 lutego 2018 r.

Grupa Robocza została powołana na mocy art. 29 dyrektywy 95/46/WE. Jest ona niezależnym europejskim organem doradczym w zakresie ochrony danych i prywatności. Zadania Grupy zostały określone w przepisach art. 30 dyrektywy 95/46/WE i art. 15 dyrektywy 2002/58/WE.

Obsługę sekretariatu zapewnia Dyrekcja C (Prawa Podstawowe i Obywatelstwo Unii Europejskiej) Dyrekcji Generalnej ds. Sprawiedliwości, B-1049 Bruksela, Belgia, biuro nr MO-59 02/013.

Strona internetowa: https://ec.europa.eu/info/law/law-topic/data-protection_pl

GRUPA ROBOCZA DS. OCHRONY OSÓB FIZYCZNYCH W ZAKRESIE PRZETWARZANIA DANYCH OSOBOWYCH

powołana na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r.,

uwzględniając art. 29 i 30 tej dyrektywy,

uwzględniając swój regulamin wewnętrzny,

PRZYJMUJE NINIEJSZE WYTYCZNE:

SPIS TREŚCI

WPROWADZENIE **5**

I. ZGŁASZANIE NARUSZENIA OCHRONY DANYCH OSOBOWYCH ZGODNIE Z RODO **6**

A. PODSTAWOWE KWESTIE DOTYCZĄCE BEZPIECZEŃSTWA 6

B. CZYM JEST NARUSZENIE OCHRONY DANYCH OSOBOWYCH? 7

1. Definicja *7*

2. Rodzaje naruszeń ochrony danych osobowych *8*

3. Potencjalne konsekwencje naruszenia ochrony danych osobowych *10*

II. ART. 33 – ZGŁASZANIE NARUSZENIA OCHRONY DANYCH OSOBOWYCH ORGANOWI NADZORCZEMU ... 11

A. KIEDY NALEŻY ZGŁOSIĆ NARUSZENIE? 11

1. Wymogi przewidziane w art. 33 ..... *11*

2. Kiedy administrator „stwierdza" wystąpienie naruszenia? *12*

3. Współadministratorzy *15*

4. Obowiązki podmiotu przetwarzającego *15*

B. UDZIELANIE INFORMACJI ORGANOWI NADZORCZEMU 16

1. Informacje, których należy udzielić *16*

2. Sukcesywne dokonywanie zgłoszenia *17*

3. Zgłoszenia dokonane z opóźnieniem *19*

C. NARUSZENIA O CHARAKTERZE TRANSGRANICZNYM I NARUSZENIA W JEDNOSTKACH ORGANIZACYJNYCH SPOZA UE 19

1. Naruszenia o charakterze transgranicznym *19*

2. Naruszenia w jednostkach organizacyjnych spoza UE *20*

D. SYTUACJE, W KTÓRYCH ZGŁASZANIE NIE JEST KONIECZNE 21

III. ART. 34 – ZAWIADAMIANIE OSOBY, KTÓREJ DANE DOTYCZĄ **23**

A. ZAWIADAMIANIE OSÓB FIZYCZNYCH 23

B. INFORMACJE, KTÓRYCH NALEŻY UDZIELIĆ 24

C. KONTAKT Z OSOBAMI FIZYCZNYMI 24

D. SYTUACJE, W KTÓRYCH ZAWIADOMIENIE NIE JEST KONIECZNE 25

IV. OCENA RYZYKA I WYSOKIEGO RYZYKA **26**

A. RYZYKO JAKO POWÓD ZGŁOSZENIA 26

B. CZYNNIKI, KTÓRE NALEŻY UWZGLĘDNIĆ PODCZAS OCENY RYZYKA 27

V. ROZLICZALNOŚĆ I PROWADZENIE DOKUMENTACJI **31**

A. DOKUMENTOWANIE NARUSZEŃ 31

B. ROLA INSPEKTORA OCHRONY DANYCH 32

VI. OBOWIĄZKI ZGŁASZANIA OKREŚLONE W INNYCH INSTRUMENTACH PRAWNYCH 33

VII. ZAŁĄCZNIK 35

A. SCHEMAT ILUSTRUJĄCY WYMOGI ZGŁASZANIA NARUSZEŃ 35

B. PRZYKŁADY NARUSZEŃ OCHRONY DANYCH OSOBOWYCH I PODMIOTÓW, KTÓRE NALEŻY POINFORMOWAĆ 36

WPROWADZENIE

W ogólnym rozporządzeniu o ochronie danych (RODO) wprowadzono wymóg zgłaszania naruszeń ochrony danych osobowych (zwanych dalej „naruszeniami") właściwemu krajowemu organowi nadzorczemu[1] (lub – w przypadku naruszeń o charakterze transgranicznym – wiodącemu organowi nadzorczemu) oraz, w określonych przypadkach, przekazywania informacji o naruszeniach osobom fizycznym, na których dane osobowe wywarły one wpływ.

Obowiązek zgłaszania przypadków naruszeń spoczywa obecnie na określonych rodzajach organizacji, np. na dostawcach publicznie dostępnych usług łączności elektronicznej (zgodnie z dyrektywą 2009/136/WE i rozporządzeniem (UE) nr 611/2013)[2]. Niektóre państwa członkowskie UE również ustanowiły już wymóg zgłaszania naruszeń w swoich własnych przepisach krajowych. Wymóg ten może wiązać się z koniecznością zgłaszania naruszeń powiązanych z określonymi kategoriami administratorów i dostawców publicznie dostępnych usług łączności elektronicznej (na przykład w Niemczech i we Włoszech) lub z koniecznością powiadamiania o wszystkich naruszeniach związanych z danymi osobowymi (na przykład w Niderlandach). Inne państwa członkowskie mogą mieć stosowne kodeksy praktyk w tym zakresie (na przykład Irlandia[3]). Choć obecnie szereg organów ochrony danych zachęca administratorów do zgłaszania naruszeń, w dyrektywie 95/46/WE o ochronie danych[4], którą RODO zastępuje, nie ustanowiono żadnego konkretnego obowiązku zgłaszania naruszeń, dlatego też wprowadzenie takiego wymogu sprawi, że wiele organizacji będzie musiało dostosować się do nowej sytuacji. Zgodnie z przepisami RODO w ich obecnym brzmieniu wszyscy administratorzy są zobowiązani do zgłaszania naruszeń, chyba że dane naruszenie najprawdopodobniej nie będzie wiązało się z ryzykiem naruszenia praw i wolności osób fizycznych[5]. Podmioty przetwarzające również mają do odegrania ważną rolę i muszą zgłaszać wszelkie naruszenia swojemu administratorowi[6].

W opinii Grupy Roboczej Art. 29 ustanowienie nowego wymogu zgłaszania naruszeń wiąże się z szeregiem korzyści. Zgłaszając naruszenie organowi nadzorczemu, administratorzy mogą zasięgnąć opinii tego organu w kwestii tego, czy w danym przypadku należy przekazać stosowne informacje osobom fizycznym, na które naruszenie wywiera wpływ. Organ nadzorczy może nakazać administratorowi, aby poinformował odpowiednie osoby fizyczne o naruszeniu[7]. Zawiadomienie osób fizycznych o naruszeniu zapewnia administratorowi możliwość przekazania tym osobom informacji na temat ryzyka związanego z naruszeniem oraz wskazania działań, jakie osoby te mogą podjąć, aby uchronić się przed potencjalnymi skutkami naruszenia. Każdy plan reagowania na naruszenia

[1] Zob. art. 4 pkt 21 RODO.

[2] Zob. https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex%3A32009L0136 i https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32013R0611

[3] Zob. https://www.dataprotection.ie/docs/Data_Security_Breach_Code_of_Practice/1082.htm

[4] Zob. https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex%3A31995L0046

[5] Prawa zapisane w Karcie praw podstawowych Unii Europejskiej dostępnej pod adresem: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A12012P%2FTXT

[6] Zob. art. 33 ust. 2. Przepis ten jest koncepcyjnie zbliżony do art. 5 rozporządzenia (UE) nr 611/2013, który stanowi, że dostawca, z którym zawarto umowę, który będzie świadczyć część usług łączności elektronicznej i który nie jest związany z abonentami bezpośrednim stosunkiem umownym, jest zobowiązany do niezwłocznego powiadomienia dostawcy zamówienia o przypadku naruszenia ochrony danych osobowych.

[7] Zob. art. 34 ust. 4 i art. 58 ust. 2 lit. e).

powinien koncentrować się przede wszystkim na zapewnieniu ochrony osobom fizycznym i ich danym osobowym. Dlatego też mechanizm zgłaszania naruszeń powinien być postrzegany jako narzędzie przyczyniające się do poprawy przestrzegania przepisów w zakresie ochrony danych osobowych. Jednocześnie należy podkreślić, że niewywiązanie się z obowiązku zgłoszenia naruszenia osobie fizycznej albo organowi nadzorczemu może potencjalnie skutkować nałożeniem na administratora kary zgodnie z art. 83.

Z tego względu administratorów i podmioty przetwarzające zachęca się do opracowywania stosownych planów z wyprzedzeniem i wdrażania procedur umożliwiających wykrywanie naruszeń i szybkie ograniczanie ich negatywnych skutków, ocenianie ryzyka dla osób fizycznych[8], a następnie podejmowanie decyzji w kwestii tego, czy w danym przypadku zachodzi konieczność zgłoszenia naruszenia właściwemu organowi nadzorczemu, jak również – w stosownych przypadkach – zawiadomienia zainteresowanych osób fizycznych o naruszeniu. Zgłoszenie naruszenia organowi nadzorczemu powinno stanowić jeden z elementów takiego planu reagowania na incydenty.

RODO zawiera przepisy określające, kiedy i komu należy zgłosić naruszenie, a także jakie informacje powinny znaleźć się w zgłoszeniu. Choć informacje, które muszą znaleźć się w zgłoszeniu, można przekazywać stopniowo, administratorzy powinni każdorazowo reagować na wszelkie naruszenia w odpowiednim czasie.

W swojej opinii 03/2014 na temat powiadamiania o przypadkach naruszenia danych osobowych[9] Grupa Robocza Art. 29 przedstawiła wytyczne dla administratorów, aby ułatwić im podjęcie decyzji w kwestii tego, czy w danym przypadku osoby, których dane dotyczą, powinny zostać zawiadomione o naruszeniu. W opinii wzięto pod uwagę obowiązki spoczywające na dostawcach usług łączności elektronicznej zgodnie z dyrektywą 2002/58/WE, zaprezentowano przykłady zaczerpnięte z wielu sektorów w kontekście RODO, które wówczas znajdowało się na etapie projektu, i przedstawiono dobre praktyki dla wszystkich administratorów.

W niniejszych wytycznych objaśniono ustanowione w RODO wymogi w zakresie obowiązkowego zgłaszania naruszeń i zawiadamiania o naruszeniach oraz omówiono niektóre działania, jakie administratorzy i podmioty przetwarzające mogą podjąć, aby należycie wywiązać się z tych nowych zobowiązań. Przedstawiono w nich również przykłady różnych rodzajów naruszeń oraz wskazano podmioty, którym w poszczególnych scenariuszach należałoby zgłosić naruszenie.

I. Zgłaszanie naruszenia ochrony danych osobowych zgodnie z RODO

A. Podstawowe kwestie dotyczące bezpieczeństwa

Zgodnie z jednym z wymogów ustanowionych w RODO dane osobowe muszą być przetwarzane za pomocą odpowiednich środków technicznych i organizacyjnych w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem[10].

[8] Można to zagwarantować w ramach wymogu dotyczącego monitorowania i przeglądu ustanowionego w ocenie skutków dla ochrony danych, której przeprowadzenie jest konieczne w przypadku operacji przetwarzania mogących powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych (art. 35 ust. 1 i 11).

[9] Zob. opinia 03/2014 na temat powiadamiania o przypadkach naruszenia danych osobowych: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp213_pl.pdf

[10] Zob. art. 5 ust. 1 lit. f) i art. 32.

Tym samym przepisy RODO zobowiązują zarówno administratorów, jak i podmioty przetwarzające do przyjęcia odpowiednich środków technicznych i organizacyjnych, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku związanemu z przetwarzaniem danych osobowych. Administratorzy i podmioty przetwarzające powinni uwzględnić stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw i wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze[11]. Ponadto w RODO ustanowiono wymóg przyjęcia wszelkich odpowiednich technicznych środków ochrony i wszelkich odpowiednich środków organizacyjnych, by od razu stwierdzić naruszenie ochrony danych osobowych, co z kolei ma decydujące znaczenie dla ustalenia, czy w danym przypadku obowiązek zgłoszenia naruszenia ma zastosowanie[12].

Oznacza to, że zdolność do zapobiegania naruszeniom w przypadkach, w których jest to możliwe, oraz zdolność do niezwłocznego reagowania na naruszenia w sytuacjach, w których mimo to dojdzie do ich wystąpienia, stanowi kluczowy element każdej polityki w zakresie bezpieczeństwa danych.

A.

B. Czym jest naruszenie ochrony danych osobowych?

1. Definicja

Podejmując jakiekolwiek działania mające na celu zaradzenie naruszeniu, administrator powinien w pierwszej kolejności potwierdzić jego wystąpienie. Termin „naruszenie ochrony danych osobowych" został zdefiniowany w art. 4 pkt 12 RODO jako:

> „naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych".

To, co należy rozumieć pod pojęciem „zniszczenia" danych osobowych, powinno być stosunkowo jasne: pojęcie to odnosi się do sytuacji, w której dane już nie istnieją lub przestały istnieć w postaci, w której administrator mógłby je w jakikolwiek sposób wykorzystać. Znaczenie pojęcia „uszkodzenie" również powinno być stosunkowo oczywiste: odnosi się ono do sytuacji, w której dane osobowe zostały zmodyfikowane, zniekształcone lub przestały być kompletne. Jeżeli chodzi o pojęcie „utraty" danych osobowych, należy interpretować je jako odnoszące się do sytuacji, w której dane mogą nadal istnieć, ale administrator utracił nad nimi kontrolę, nie posiada już do nich dostępu lub nie znajduje się już w ich posiadaniu. Nieuprawnione lub niezgodne z prawem przetwarzanie może oznaczać ujawnienie (lub udostępnienie) danych osobowych odbiorcom, którzy nie są upoważnieni do ich otrzymania (lub do uzyskania do nich dostępu), lub jakąkolwiek inną formę przetwarzania skutkującą naruszeniem przepisów RODO.

Przykład

Przykładem utraty danych osobowych może być sytuacja, w której dochodzi do utraty lub kradzieży urządzenia, na którym przechowywana jest kopia bazy danych klientów administratora. Kolejnym przykładem zdarzenia skutkującego utratą danych może być również sytuacja, w której jedyna kopia zbioru danych osobowych została zaszyfrowana wskutek zastosowania oprogramowania typu

[11] Art. 32; zob. również motyw 83.

[12] Zob. motyw 87.

ransomware, lub sytuacja, w której administrator zaszyfrował dane za pomocą klucza, który nie znajduje się już w jego posiadaniu.

W tym kontekście należy podkreślić, że naruszenie jest rodzajem incydentu bezpieczeństwa. Jak jednak wskazano w art. 4 pkt 12, przepisy RODO mają zastosowanie wyłącznie w przypadku, gdy dochodzi do naruszenia ochrony *danych osobowych*. Wystąpienie takiego naruszenia prowadzi do sytuacji, w której administrator nie jest w stanie zapewnić zgodności z zasadami dotyczącymi przetwarzania danych osobowych ustanowionymi w art. 5 RODO. Stanowi to element pozwalający odróżnić incydent bezpieczeństwa od zdarzenia skutkującego naruszeniem ochrony danych osobowych – co do zasady, choć wszystkie przypadki naruszenia ochrony danych osobowych są incydentami bezpieczeństwa, nie wszystkie incydenty bezpieczeństwa muszą wiązać się z naruszeniem ochrony danych osobowych[13].

Poniżej omówiono potencjalne negatywne skutki naruszenia ochrony danych osobowych dla osób fizycznych.

2. Rodzaje naruszeń ochrony danych osobowych

W swojej opinii 03/2014 na temat powiadamiania o przypadkach naruszenia Grupa Robocza Art. 29 wyjaśniła, że zgodnie z trzema powszechnie uznawanymi zasadami bezpieczeństwa[14] naruszenia można podzielić na następujące kategorie:

- „naruszenie dotyczące poufności danych" – naruszenie, w rezultacie którego dochodzi do nieuprawnionego lub przypadkowego ujawnienia lub nieuprawnionego dostępu do danych osobowych;
- „naruszenie dotyczące integralności danych" – naruszenie, w rezultacie którego dochodzi do nieuprawnionego lub przypadkowego zmodyfikowania danych osobowych;
- „naruszenie dotyczące dostępności danych" – naruszenie, w rezultacie którego dochodzi do przypadkowego lub nieuprawnionego dostępu[15] do danych osobowych lub zniszczenia danych osobowych.

Należy również podkreślić, że – w zależności od okoliczności – naruszenie może dotyczyć jednocześnie poufności, integralności i dostępności danych, a także dowolnego połączenia dwóch spośród tych trzech kategorii naruszeń.

Choć ustalenie, czy w danym przypadku doszło do naruszenia dotyczącego poufności lub integralności danych, jest stosunkowo łatwe, stwierdzenie wystąpienia naruszenia dotyczącego dostępności danych może okazać się trudniejsze. Naruszenie zostanie każdorazowo uznane za

[13] Należy podkreślić, że zakres pojęcia „incydent bezpieczeństwa" nie ogranicza się wyłącznie do modeli zagrożeń, w których źródło ataku na organizację znajduje się poza organizacją, ale obejmuje również incydenty związane z przetwarzaniem danych wewnątrz organizacji w sposób naruszający zasady bezpieczeństwa.

[14] Zob. opinia 03/2014.

[15] Powszechnie przyjmuje się, że pojęcie „dostępu" stanowi zasadniczo element pojęcia „dostępności". Zob. na przykład dokument NIST SP800-53rev4, w którym przedstawiono następującą definicję terminu „dostępność": „zapewnienie możliwości uzyskania terminowego i niezawodnego dostępu do informacji oraz możliwości terminowego i niezawodnego korzystania z informacji"; dokument jest dostępny pod adresem: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf . W dokumencie CNSSI-4009 wspomina się również o: „terminowym i niezawodnym dostępie do usług w zakresie danych i informacji dla upoważnionych użytkowników". Zob. https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf. Również w normie ISO/IEC 27000:2016 „dostępność" zdefiniowano jako „właściwość polegającą na tym, że cechujący się nią obiekt jest dostępny i gotowy do wykorzystania na żądanie uprawnionego podmiotu": https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-4:v1:en

naruszenie dotyczące dostępności danych, jeżeli doprowadziło ono do trwałej utraty lub zniszczenia danych osobowych.

Przykład

Przykłady utraty dostępności obejmują sytuacje, w których doszło do przypadkowego usunięcia danych albo ich usunięcia przez nieuprawnioną osobę, lub – w przypadku bezpiecznie zaszyfrowanych danych – sytuacje, w których utracono klucz deszyfrujący. Sytuację, w której administrator nie jest w stanie przywrócić dostępu do danych, na przykład korzystając z kopii bezpieczeństwa, uznaje się za sytuację, w której doszło do trwałej utraty dostępności.

Do utraty dostępności może dojść również w przypadku poważnego zakłócenia normalnego sposobu funkcjonowania organizacji, np. wskutek awarii systemu zasilania lub ataku typu „odmowa usługi", skutkującego utratą dostępu do danych osobowych.

W tym kontekście warto zastanowić się nad tym, czy tymczasowa utrata dostępności danych osobowych powinna zostać uznana za sytuację, w której doszło do wystąpienia naruszenia, a jeżeli tak – czy naruszenie to należy zgłosić. W art. 32 RODO zatytułowanym „Bezpieczeństwo przetwarzania" wyjaśniono, że przy wdrażaniu środków technicznych i organizacyjnych pozwalających zapewnić stopień bezpieczeństwa odpowiadający ryzyku, należy wziąć pod uwagę m.in. „zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania" oraz „zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego".

Dlatego też incydent bezpieczeństwa skutkujący utratą dostępu do danych osobowych przez określony czas również stanowi rodzaj naruszenia, ponieważ brak dostępu do danych może wywrzeć istotny wpływ na prawa i wolności osób fizycznych. Gwoli wyjaśnienia, jeżeli dane osobowe są niedostępne z uwagi na fakt, że system jest poddawany wcześniej zaplanowanym pracom konserwacyjnym, taka sytuacja nie stanowi przypadku „naruszenia bezpieczeństwa", o którym mowa w definicji ustanowionej w art. 4 pkt 12.

Naruszenie skutkujące tymczasową utratą dostępności danych powinno zostać udokumentowane zgodnie z art. 33 ust. 5, podobnie jak naruszenie skutkujące trwałą utratą lub zniszczeniem danych osobowych (lub dowolny inny rodzaj naruszenia). Ułatwi to administratorowi wykazanie rozliczalności przed organem nadzorczym, który może zwrócić się o udostępnienie mu rejestrów do wglądu[16]. W zależności od specyfiki danego naruszenia konieczne może jednak okazać się zgłoszenie go organowi nadzorczemu lub zawiadomienie o jego wystąpieniu osób fizycznych, na które wywiera ono wpływ. Administrator będzie musiał ocenić prawdopodobieństwo wystąpienia i wagę wpływu na prawa i wolności osób fizycznych w związku z brakiem dostępności danych osobowych. Zgodnie z art. 33 administrator jest zobowiązany do zgłoszenia naruszenia, chyba że dane naruszenie najprawdopodobniej nie będzie wiązało się z ryzykiem naruszenia praw i wolności osób fizycznych. Kwestię tę trzeba będzie oczywiście ocenić w poszczególnych przypadkach.

Przykłady

Utrata dostępu do kluczowych danych medycznych w szpitalu – nawet jeżeli ma wyłącznie tymczasowy charakter – może wiązać się z ryzykiem naruszenia praw i wolności osób fizycznych; wystąpienie takiej sytuacji może np. wiązać się z koniecznością odwołania operacji, co stwarza zagrożenie dla życia pacjentów.

[16] Zob. art. 33 ust. 5.

Z kolei jeżeli przedsiębiorstwo medialne nie mogło przesłać swoim subskrybentom biuletynów informacyjnych z uwagi na kilkugodzinną utratę dostępu do swoich systemów (np. z powodu awarii systemu zasilania), prawdopodobieństwo, że taka sytuacja będzie wiązała się z ryzykiem naruszenia prawa i wolności osób fizycznych, jest niewielkie.

Należy podkreślić, że choć utrata dostępu do systemów administratora może mieć wyłącznie tymczasowy charakter i może nie wywierać wpływu na osoby fizyczne, administrator powinien wziąć pod uwagę wszystkie potencjalne konsekwencje naruszenia, ponieważ może ono nadal wymagać zgłoszenia z innych względów.

Przykład

Zainfekowanie oprogramowaniem typu ransomware (złośliwym oprogramowaniem, które szyfruje dane administratora do momentu zapłacenia okupu) mogłoby doprowadzić do tymczasowej utraty dostępności, jeżeli w danym przypadku możliwe byłoby przywrócenie danych z kopii bezpieczeństwa. Nie zmienia to jednak faktu, że włamanie do sieci miało miejsce i może podlegać obowiązkowi zgłoszenia, jeżeli dany incydent zostanie uznany za naruszenie dotyczące poufności danych (tj. jeżeli hakerowi udało się uzyskać dostęp do danych osobowych) i wiąże się z ryzykiem naruszenia praw i wolności osób fizycznych.

3. Potencjalne konsekwencje naruszenia ochrony danych osobowych

Naruszenie może potencjalnie wywrzeć szereg negatywnych skutków dla osób fizycznych, które mogą skutkować powstaniem uszczerbku fizycznego, szkód majątkowych lub szkód niemajątkowych. W RODO wyjaśniono, że takie skutki mogą obejmować utratę kontroli nad własnymi danymi osobowymi, ograniczenie praw, dyskryminację, kradzież lub sfałszowanie tożsamości, stratę finansową, nieuprawnione odwrócenie pseudonimizacji, naruszenie dobrego imienia oraz naruszenie poufności danych osobowych chronionych tajemnicą zawodową. Mogą one również wiązać się z wszelkimi innymi znacznymi szkodami gospodarczymi lub społecznymi dla tych osób fizycznych[17].

Dlatego też w RODO ustanowiono wymóg zobowiązujący administratora do zgłoszenia naruszenia właściwemu organowi nadzorczemu, chyba że dane naruszenie najprawdopodobniej nie będzie wiązało się z ryzykiem wywołania takich negatywnych skutków. Jeżeli w danym przypadku istnieje duże ryzyko wystąpienia negatywnych skutków, przepisy RODO zobowiązują administratora do przekazania informacji o naruszeniu osobom fizycznym, na które wywiera ono wpływ, tak szybko, jak będzie to rozsądnie możliwe[18].

Znaczenie zdolności do określenia, czy w danym przypadku doszło do naruszenia, ocenienia ryzyka dla osób fizycznych oraz późniejszego zgłoszenia naruszenia w przypadkach, w których będzie to konieczne, podkreślono w motywie 87 RODO:

„Należy się upewnić, czy wdrożono wszelkie odpowiednie techniczne środki ochrony i wszelkie odpowiednie środki organizacyjne, by od razu stwierdzić naruszenie ochrony danych osobowych i szybko poinformować organ nadzorczy i osobę, której dane dotyczą. To, czy zawiadomienia dokonano bez zbędnej zwłoki, należy ustalić z uwzględnieniem w szczególności charakteru i wagi naruszenia ochrony danych osobowych, jego konsekwencji oraz niekorzystnych skutków dla osoby, której dane dotyczą. Takie zawiadomienie może skutkować interwencją organu nadzorczego, zgodnie z jego zadaniami i uprawnieniami określonymi w niniejszym rozporządzeniu”.

[17] Zob. również motywy 85 i 75.

[18] Zob. również motyw 86.

Dalsze wytyczne dotyczące oceny ryzyka negatywnych skutków dla osób fizycznych przedstawiono w sekcji IV.

Jeżeli administratorzy nie wywiążą się z obowiązku zgłoszenia naruszenia ochrony danych organowi nadzorczemu albo osobom, których dane dotyczą, albo zarówno organowi nadzorczemu, jak i osobom, których dane dotyczą, pomimo spełnienia wymogów ustanowionych w art. 33 lub 34, organ nadzorczy może skorzystać z możliwości, która obejmowałaby wzięcie pod uwagę wszystkich środków naprawczych znajdujących się do jego dyspozycji, co wiązałoby się z możliwością zastosowania administracyjnej kary pieniężnej[19] w połączeniu ze środkiem naprawczym przewidzianym w art. 58 ust. 2 albo bez takiego środka. Jeżeli zdecydowano się zastosować administracyjną karę pieniężną, wartość tej kary może opiewać na kwotę do 10 000 000 EUR lub do 2 % całkowitego rocznego światowego obrotu przedsiębiorstwa zgodnie z art. 83 ust. 4 lit. a) RODO. Należy również pamiętać o tym, że w niektórych przypadkach niewywiązanie się z obowiązku zgłoszenia naruszenia mogłoby doprowadzić do ujawnienia braku istniejących środków bezpieczeństwa albo nieadekwatności istniejących środków bezpieczeństwa. Wytyczne Grupy Roboczej Art. 29 w sprawie administracyjnych kar pieniężnych stanowią, że: „występowanie kilku różnych naruszeń popełnionych łącznie w konkretnym pojedynczym przypadku oznacza, że organ nadzorczy może nakładać administracyjne kary pieniężne w sposób, który jest zarazem skuteczny, proporcjonalny i odstraszający na poziomie najpoważniejszego naruszenia”. W takim przypadku organ nadzorczy będzie miał również możliwość nakładania kar za niewywiązanie się z obowiązku zgłoszenia naruszenia lub zawiadomienia o wystąpieniu naruszenia (art. 33 i 34), z jednej strony, oraz za brak (odpowiednich) środków bezpieczeństwa (art. 32), z drugiej strony, ponieważ obydwie te sytuacje traktuje się jako dwa odrębne naruszenia.

II. Art. 33 – Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu

A. Kiedy należy zgłosić naruszenie?

1. Wymogi przewidziane w art. 33

Art. 33 ust. 1 stanowi, że:

„W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia”.

Motyw 87 stanowi, że[20]:

„Należy się upewnić, czy wdrożono wszelkie odpowiednie techniczne środki ochrony i wszelkie odpowiednie środki organizacyjne, by od razu stwierdzić naruszenie ochrony danych osobowych i szybko poinformować organ nadzorczy i osobę, której dane dotyczą. To, czy zawiadomienia

[19] Aby uzyskać dalsze szczegółowe informacje, zob. wytyczne Grupy Roboczej Art. 29 w sprawie stosowania i ustalania administracyjnych kar pieniężnych dostępne pod adresem: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237

[20] W tym kontekście istotne znaczenie ma również motyw 85.

dokonano bez zbędnej zwłoki, należy ustalić z uwzględnieniem w szczególności charakteru i wagi naruszenia ochrony danych osobowych, jego konsekwencji oraz niekorzystnych skutków dla osoby, której dane dotyczą. Takie zawiadomienie może skutkować interwencją organu nadzorczego, zgodnie z jego zadaniami i uprawnieniami określonymi w niniejszym rozporządzeniu".

2. Kiedy administrator „stwierdza" wystąpienie naruszenia?

Jak wyszczególniono powyżej, w RODO ustanowiono wymóg, zgodnie z którym w przypadku naruszenia ochrony danych osobowych administrator bez zbędnej zwłoki – w miarę możliwości nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu. Stosowanie tego wymogu może wiązać się z koniecznością ustalenia momentu, w którym można uznać, że administrator „stwierdził" wystąpienie naruszenia. W opinii Grupy Roboczej Art. 29 należy uznać, że administrator „stwierdził" wystąpienie naruszenia w momencie, w którym uzyskał wystarczającą dozą pewności co do tego, że doszło do wystąpienia incydentu bezpieczeństwa, który doprowadził do ujawnienia danych osobowych.

Jak jednak wspomniano wcześniej, w RODO ustanowiono wymóg zobowiązujący administratora do wdrożenia wszelkich odpowiednich technicznych środków ochrony i wszelkich odpowiednich środków organizacyjnych, by od razu stwierdzić naruszenie ochrony danych osobowych i szybko poinformować organ nadzorczy i osoby, których dane dotyczą. W RODO stwierdzono również, że to, czy zawiadomienia dokonano bez zbędnej zwłoki, należy ustalić z uwzględnieniem w szczególności charakteru i wagi naruszenia ochrony danych osobowych, jego konsekwencji oraz niekorzystnych skutków dla osoby, której dane dotyczą[21]. Wiąże się to z nałożeniem na administratora obowiązku utrzymania zdolności do terminowego „stwierdzania" wystąpienia wszelkich naruszeń, aby zapewnić możliwość podjęcia stosownych działań.

To, kiedy dokładnie można uznać, że administrator „stwierdził" wystąpienie określonego naruszenia, będzie zależało od okoliczności, w jakich doszło do tego naruszenia. W niektórych przypadkach wystąpienie naruszenia można stosunkowo łatwo stwierdzić już na początku, natomiast w innych ustalenie, czy doszło do ujawnienia danych osobowych, może wymagać czasu. W tym kontekście powinno się jednak położyć nacisk na szybkie zbadanie danego incydentu w celu ustalenia, czy faktycznie doszło do naruszenia ochrony danych osobowych, a jeżeli tak – podjąć działania zaradcze i, w razie konieczności, zgłosić naruszenie.

Przykłady

1. W przypadku utraty pamięci USB zawierającej niezaszyfrowane dane osobowe ustalenie, czy nieuprawnione osoby uzyskały dostęp do tych danych, okazuje się często niemożliwe. Niemniej jednak, mimo że administrator może nie być w stanie ustalić, czy w danym przypadku doszło do naruszenia dotyczącego poufności danych, taki przypadek musi zostać zgłoszony, ponieważ można z wystarczającą dozą pewności stwierdzić, że doszło do naruszenia dotyczącego dostępności danych; w tym kontekście przyjmuje się, że administrator „stwierdził" wystąpienie naruszenia w momencie, w którym zdał sobie sprawę z utraty pamięci USB.

2. Osoba trzecia informuje administratora, że przypadkowo otrzymała dane osobowe jednego z jego klientów, i przedstawia dowody potwierdzające, że doszło do nieuprawnionego ujawnienia tych danych. Ponieważ administrator otrzymał dowody jednoznacznie świadczące o wystąpieniu naruszenia dotyczącego poufności danych, nie można mieć żadnych wątpliwości co do tego, że „stwierdził" wystąpienie takiego naruszenia.

[21] Zob. motyw 87.

3. Administrator wykrywa potencjalne włamanie do swojej sieci. Administrator sprawdza systemy w celu ustalenia, czy bezpieczeństwo danych osobowych przechowywanych w tym systemie zostało narażone na szwank, po czym potwierdza, że faktycznie tak się stało. Ponownie, ponieważ administrator uzyskał dowody jednoznacznie świadczące o wystąpieniu naruszenia, nie można mieć żadnych wątpliwości co do tego, że „stwierdził" wystąpienie takiego naruszenia.

4. Cyberprzestępca kontaktuje się z administratorem po włamaniu się do jego systemu, aby zażądać okupu. W takim przypadku – po sprawdzeniu swojego systemu i potwierdzeniu, że faktycznie został on zaatakowany – administrator dysponuje dowodem jednoznacznie świadczącym o wystąpieniu naruszenia, dlatego też nie można mieć żadnych wątpliwości co do tego, że stwierdził wystąpienie takiego naruszenia.

Po otrzymaniu pierwszej informacji o potencjalnym naruszeniu ochrony danych osobowych od osoby fizycznej, organizacji medialnej lub z innego źródła lub po samodzielnym wykryciu incydentu bezpieczeństwa administrator może przeprowadzić krótkotrwałe postępowanie, aby ustalić, czy faktycznie doszło do danego naruszenia. Do momentu zakończenia tego postępowania nie można uznać, że administrator „stwierdził" wystąpienie naruszenia. Oczekuje się jednak, że wstępne postępowanie powinno rozpocząć się możliwie jak najszybciej i doprowadzić do ustalenia z wystarczającą dozą pewności, czy w danym przypadku faktycznie doszło do wystąpienia naruszenia; następnie można przeprowadzić bardziej szczegółowe postępowanie.

Po stwierdzeniu wystąpienia naruszenia przez administratora podlegające zgłoszeniu naruszenie musi zostać zgłoszone bez zbędnej zwłoki, w miarę możliwości nie później niż w terminie 72 godzin po stwierdzeniu naruszenia. W tym okresie administrator powinien ocenić prawdopodobne ryzyko, na jakie narażone są osoby fizyczne, aby ustalić, czy w danym przypadku zastosowanie ma wymóg zgłoszenia naruszenia, a także aby określić działanie lub działania, które należy podjąć, aby zaradzić naruszeniu. Administrator mógł już jednak przeprowadzić wstępną ocenę potencjalnego ryzyka, z jakim może wiązać się naruszenie, w ramach oceny skutków dla ochrony danych[22] dokonanej przed przeprowadzeniem danej operacji przetwarzania. Ocena skutków dla ochrony danych może mieć jednak bardziej ogólnikowy charakter niż ocena konkretnych okoliczności, w których doszło do dowolnego faktycznego naruszenia, dlatego też należy również każdorazowo przeprowadzić dodatkową ocenę uwzględniającą te okoliczności. Aby uzyskać bardziej szczegółowe informacje na temat oceny ryzyka, zob. sekcja IV.

W większości przypadków takie wstępne działania powinny zostać zakończone wkrótce po otrzymaniu początkowego ostrzeżenia (tj. w momencie powzięcia przez administratora lub podmiot przetwarzający podejrzenia o możliwości wystąpienia incydentu bezpieczeństwa mogącego wywrzeć wpływ na dane osobowe) – działania te mogą zostać zakończone w późniejszym terminie wyłącznie w wyjątkowych przypadkach.

Przykład

Osoba fizyczna informuje administratora, że otrzymała wiadomość e-mail, której nadawca podszywa się pod administratora i która zawiera dane osobowe dotyczące (faktycznego) korzystania z usług administratora przez tę osobę, i sugeruje, że doszło do złamania środków bezpieczeństwa stosowanych przez administratora. Administrator przeprowadza krótkie postępowanie, w toku którego uzyskuje potwierdzenie, że doszło do włamania do jego sieci, i gromadzi dowody świadczące o nieuprawnionym dostępie do danych osobowych. Od tego momentu przyjmuje się, że administrator

[22] Zob. wytyczne Grupy Roboczej Art. 29 dotyczące oceny skutków dla ochrony danych: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

„stwierdził" wystąpienie naruszenia, a zgłoszenie naruszenia organowi nadzorczemu staje się obowiązkowe, chyba że prawdopodobieństwo, iż będzie wiązało się ono z ryzykiem naruszenia praw i wolności osób fizycznych, jest niewielkie. Administrator będzie musiał podjąć odpowiednie działania zaradcze, aby zaradzić naruszeniu.

Dlatego też administrator powinien ustanowić wewnętrzne procedury zapewniające mu możliwość wykrycia naruszenia i zaradzenia mu. Na przykład, aby wykryć pewne nieprawidłowości w procesie przetwarzania danych, administrator lub podmiot przetwarzający mogą korzystać z określonych środków technicznych takich jak analizatory przepływu danych i analizatory dziennika umożliwiające zidentyfikowanie zdarzeń i ostrzeżeń poprzez ich zestawienie z dowolnymi danymi dziennika[23]. Po wykryciu naruszenia należy powiadomić o jego wystąpieniu organ zarządzający wyższego szczebla, aby można było mu zaradzić i – w razie potrzeby – zgłosić je zgodnie z art. 33 oraz, w stosownych przypadkach, art. 34. Takie środki i mechanizmy zgłaszania powinny zostać szczegółowo opisane w sporządzonych przez administratora planach reagowania na incydenty lub w przyjętych przez niego zasadach zarządzania. Ułatwi to administratorowi efektywne planowanie działań i ustalenie podmiotów w organizacji, na których spoczywa odpowiedzialność operacyjna za zarządzanie naruszeniem, a także określenie – w stosownych przypadkach – czy lub w jaki sposób powiadomić organ zarządzający wyższego szczebla o wystąpieniu danego incydentu.

Administrator powinien również zawrzeć porozumienia ze wszystkimi podmiotami przetwarzającymi, z których usług korzysta – podmioty te są z kolei zobowiązane do zgłaszania administratorowi przypadków wystąpienia naruszenia (zob. poniżej).

Choć odpowiedzialność za ustanawianie odpowiednich środków umożliwiających przeciwdziałanie naruszeniom, reagowanie na naruszenia i zaradzanie im spoczywa na administratorach i podmiotach przetwarzających, istnieją pewne praktyczne działania, które powinny być podejmowane we wszystkich przypadkach:

- informacje na temat wszystkich zdarzeń powiązanych z bezpieczeństwem powinny być przekazywane osobie lub osobom, którym powierzono zadanie reagowania na incydenty, ustalania istnienia naruszenia i oceniania poziomu ryzyka;
- następnie należy ocenić ryzyko dla osób fizycznych związane z danym naruszeniem (prawdopodobieństwo braku ryzyka, istnienie ryzyka lub wysoki poziom ryzyka) oraz przekazać stosowne informacje w tym zakresie odpowiednim działom w ramach danej organizacji;
- w razie konieczności należy zgłosić dane naruszenie organowi nadzorczemu oraz, potencjalnie, poinformować o naruszeniu osoby fizyczne, na które wywarło ono wpływ;
- jednocześnie administrator powinien podjąć działania mające na celu ograniczenie skali naruszenia i przywrócenie stanu sprzed wystąpienia naruszenia;
- informacje na temat naruszenia powinny być dokumentowane w miarę rozwoju sytuacji.

Tym samym na administratorze spoczywa wyraźny obowiązek podejmowania działań w związku z wszelkimi ostrzeżeniami otrzymanymi na początkowym etapie oraz obowiązek ustalenia, czy w danym przypadku faktycznie doszło do naruszenia, czy też nie. W tym krótkim okresie administrator może przeprowadzić pewne postępowania oraz zgromadzić dowody i inne istotne szczegółowe informacje. Jednak po tym, gdy administrator z wystarczającą dozą pewności stwierdzi, że w danym przypadku doszło do naruszenia – i jeżeli spełnione zostały warunki ustanowione w art. 33 ust. 1 – musi zgłosić dane naruszenie organowi nadzorczemu bez zbędnej zwłoki, w miarę możliwości nie później niż w terminie 72 godzin[24]. Jeżeli administrator nie wywiąże się z obowiązku podjęcia działań w odpowiednim terminie, a okoliczności danej sprawy będą jednoznacznie wskazywały na to, że doszło do naruszenia, taka sytuacja może zostać uznana za przypadek niewywiązania się z obowiązku zgłoszenia naruszenia zgodnie z art. 33.

Z art. 32 jednoznacznie wynika, że administrator i podmiot przetwarzający powinni dysponować odpowiednimi środkami technicznymi i organizacyjnymi, aby zapewnić odpowiedni stopień bezpieczeństwa danych osobowych: zdolność do wykrywania naruszeń, zaradzania im oraz ich terminowego zgłaszania powinna być postrzegana jako kluczowy element tych środków.

3. Współadministratorzy

Art. 26 dotyczy współadministratorów i stanowi, że współadministratorzy określają zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z RODO[25]. Wiąże się to z koniecznością ustalenia, która strona będzie odpowiedzialna za wywiązywanie się z zobowiązań ustanowionych w art. 33 i 34. Grupa Robocza Art. 29 zaleca, aby uzgodnienia umowne między współadministratorami uwzględniały postanowienia wskazujące administratora, który będzie zajmował się dbaniem o wypełnianie ustanowionych w RODO obowiązków w zakresie zgłaszania naruszeń lub który będzie odpowiedzialny za wypełnianie tych obowiązków.

4. Obowiązki podmiotu przetwarzającego

Choć ogólna odpowiedzialność za dbanie o ochronę danych osobowych spoczywa na administratorze, podmiot przetwarzający odgrywa istotną rolę w zapewnianiu administratorowi możliwości wywiązania się ze spoczywających na nim obowiązków; obejmuje to również zgłaszanie naruszeń. W art. 28 ust. 3 stwierdzono, że przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy lub innego instrumentu prawnego. Zgodnie z art. 28 ust. 3 lit. f) umowa lub inny instrument prawny stanowią w szczególności, że podmiot przetwarzający: „uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi wywiązać się z obowiązków określonych w art. 32–36".

W art. 33 ust. 2 wskazano wyraźnie, że w przypadku, gdy administrator korzysta z usług podmiotu przetwarzającego, a podmiot przetwarzający stwierdzi wystąpienie naruszenia ochrony danych osobowych, które przetwarza w imieniu administratora, musi zgłosić to naruszenie administratorowi „bez zbędnej zwłoki". Należy przy tym podkreślić, że podmiot przetwarzający nie musi ocenić prawdopodobieństwa wystąpienia ryzyka wynikającego z naruszenia przed jego zgłoszeniem administratorowi; odpowiedzialność za przeprowadzenie takiej oceny w momencie stwierdzenia wystąpienia naruszenia spoczywa na administratorze. Podmiot przetwarzający musi jedynie ustalić, czy doszło do naruszenia, a następnie zgłosić to naruszenie administratorowi. Administrator korzysta z usług podmiotu przetwarzającego, aby realizować wyznaczone cele; dlatego też zasadniczo należy przyjąć, że administrator „stwierdził" wystąpienie naruszenia w momencie, w którym podmiot przetwarzający poinformował go o jego wystąpieniu. Nałożenie na podmiot przetwarzający obowiązku zgłoszenia naruszenia administratorowi, na rzecz którego podmiot ten świadczy usługi, zapewnia temu administratorowi możliwość zaradzenia naruszeniu i ustalenia, czy w danym przypadku należy zgłosić to naruszenie organowi nadzorczemu zgodnie z art. 33 ust. 1 oraz zawiadomić o jego wystąpieniu osoby fizyczne, na które naruszenie wywiera wpływ, zgodnie z art. 34 ust. 1. Administrator może również zdecydować się na przeprowadzenie postępowania w sprawie

[23] Należy podkreślić, że dane dziennika ułatwiające audytowanie, np. dane dotyczące przechowywania, modyfikowania lub usuwania danych, mogą być również zaklasyfikowane jako dane osobowe dotyczące osoby, która wszczęła daną operację przetwarzania.

[24] Zob. rozporządzenie nr 1182/71 określające zasady mające zastosowanie do okresów, dat i terminów dostępne pod adresem: https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:31971R1182&from=EN

[25] Zob. również motyw 79.

naruszenia, ponieważ może nie dysponować wiedzą na temat wszystkich istotnych okoliczności faktycznych danej sprawy – na przykład tego, czy w posiadaniu administratora znajduje się kopia lub kopia bezpieczeństwa danych osobowych zniszczonych lub utraconych przez podmiot przetwarzający. Może to decydować o tym, czy administrator musiałby następnie zgłosić naruszenie.

W RODO nie ustanowiono precyzyjnie określonego terminu, w którym podmiot przetwarzający musi zgłosić naruszenie administratorowi – stwierdzono jedynie, że musi to nastąpić „bez zbędnej zwłoki". Dlatego też Grupa Robocza Art. 29 zaleca, aby podmiot przetwarzający szybko zgłaszał naruszenia administratorowi i następnie stopniowo przekazywał dalsze informacje na temat naruszenia, w miarę uzyskiwania dostępu do bardziej szczegółowych danych. Ma to istotne znaczenie dla ułatwienia administratorowi spełnienia wymogu zgłoszenia naruszenia organowi nadzorczemu w terminie 72 godzin.

Jak wyjaśniono powyżej, w umowie między administratorem a podmiotem przetwarzającym należy określić, w jaki sposób planuje się zagwarantować spełnienie wymogów ustanowionych w art. 33 ust. 2 oraz zapewnić zgodność z innymi przepisami RODO. Może wiązać się to z ustanowieniem obowiązku wczesnego zgłaszania naruszeń przez podmiot przetwarzający, co z kolei ułatwia administratorowi wywiązanie się ze spoczywających na nim obowiązków w zakresie zgłaszania naruszeń organowi nadzorczemu w terminie 72 godzin.

Jeżeli podmiot przetwarzający świadczy usługi na rzecz szeregu administratorów, a dany incydent wywiera wpływ na wszystkich z nich, podmiot przetwarzający będzie zobowiązany do zgłoszenia wystąpienia wspomnianego incydentu każdemu z tych administratorów.

Podmiot przetwarzający mógłby dokonać zgłoszenia w imieniu administratora, jeżeli administrator udzieliłby takiemu podmiotowi przetwarzającemu stosownego zezwolenia, a kwestia ta zostałaby uregulowana w uzgodnieniach umownych między administratorem a podmiotem przetwarzającym. Takiego zgłoszenia należy dokonać zgodnie z art. 33 i 34. W tym kontekście należy jednak pamiętać, że zgodnie z obowiązującymi przepisami odpowiedzialność za dokonanie zgłoszenia spoczywa na administratorze.

B. Udzielanie informacji organowi nadzorczemu

1. Informacje, których należy udzielić

Art. 33 ust. 3 stanowi, że w przypadku, gdy administrator zgłasza naruszenie organowi nadzorczemu, zgłoszenie to powinno co najmniej:

„a) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;

b) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;

c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;

d) opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków".

W RODO nie zawarto definicji kategorii osób, których dane dotyczą, ani kategorii wpisów danych osobowych. Grupa Robocza Art. 29 zaproponowała jednak kategorie osób, których dane dotyczą, obejmujące różnego rodzaju osoby fizyczne, na których dane osobowe naruszenie wywarło wpływ: w zależności od zastosowanych wskaźników kategorie te mogą obejmować m.in. dzieci

i przedstawicieli innych grup szczególnie wrażliwych, osoby niepełnosprawne, pracowników lub klientów. Podobnie kategorie wpisów danych osobowych mogą odnosić się do poszczególnych rodzajów wpisów, które administrator może przetwarzać, takich jak dane dotyczące zdrowia, dane dotyczące wykształcenia, informacje z dziedziny opieki społecznej, szczegółowe informacje finansowe, numery rachunków bankowych, numery paszportów itp.

W motywie 85 wyraźnie stwierdzono, że jednym z powodów, dla których zgłasza się naruszenie, jest ograniczenie związanych z nim szkód dla osób fizycznych. Dlatego też jeżeli rodzaje osób, których dane dotyczą, lub rodzaje danych osobowych wskazują na istnienie ryzyka wyrządzenia określonych szkód w rezultacie naruszenia (np. kradzież tożsamości, oszustwo, strata finansowa, ryzyko naruszenia poufności danych chronionych tajemnicą zawodową), należy wskazać stosowne kategorie w zgłoszeniu. Pozwoli to spełnić wymóg opisania możliwych konsekwencji naruszenia.

Brak dostępu do szczegółowych informacji (np. informacji o dokładnej liczbie osób, których dane dotyczą, na które naruszenie wywarło wpływ) nie powinien stanowić przeszkody dla terminowego zgłoszenia naruszenia. Przepisy RODO dopuszczają możliwość wskazywania przybliżonej liczby osób fizycznych, na które dane naruszenie wywarło wpływ, oraz przybliżonej liczby wpisów danych osobowych, których dotyczy to naruszenie. W tym kontekście należy skoncentrować się na dążeniu do zaradzenia negatywnym skutkom naruszenia, a nie na przedstawieniu precyzyjnych danych liczbowych. Dlatego też w przypadku, w którym fakt wystąpienia naruszenia nie wzbudza żadnych wątpliwości, ale jego skala nie jest jeszcze znana, sukcesywne dokonywanie zgłoszenia (zob. poniżej) stanowi bezpieczną metodę wywiązania się z zobowiązań w zakresie zgłaszania naruszeń.

Art. 33 ust. 3 stanowi, że administrator „musi co najmniej" przekazać tego rodzaju informacje w zgłoszeniu, aby – w stosownych przypadkach – mieć możliwość przekazania dodatkowych szczegółowych informacji na późniejszym etapie. Różne rodzaje naruszeń (dotyczące poufności, integralności lub dostępności) mogą wiązać się z koniecznością przekazania dodatkowych informacji, aby w pełni wyjaśnić okoliczności danej sprawy.

Przykład

W zgłoszeniu skierowanym do organu nadzorczego administrator może podać nazwę swojego podmiotu przetwarzającego, jeżeli do danego naruszenia doszło na poziomie takiego podmiotu, a w szczególności jeżeli naruszenie doprowadziło do incydentu wywierającego wpływ na wpisy danych osobowych wielu innych administratorów, którzy korzystają z usług tego samego podmiotu przetwarzającego.

Niezależnie od danego przypadku organ nadzorczy może zwrócić się o udzielenie mu dalszych szczegółowych informacji w ramach prowadzonego przez siebie postępowania w przedmiocie naruszenia.

2. Sukcesywne dokonywanie zgłoszenia

W zależności od charakteru danego naruszenia ustalenie wszystkich istotnych okoliczności faktycznych związanych z incydentem może wiązać się z koniecznością przeprowadzenia bardziej szczegółowego postępowania przez administratora. Dlatego też art. 33 ust. 4 stanowi:

„Jeżeli – i w zakresie, w jakim – informacji nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki".

Oznacza to, że w RODO uznaje się, iż administratorzy nie zawsze są w stanie uzyskać dostęp do wszystkich niezbędnych informacji na temat naruszenia w ciągu 72 godzin od stwierdzenia wystąpienia naruszenia, ponieważ pełne i wyczerpujące szczegółowe informacje na temat danego incydentu nie zawsze są dostępne w tym początkowym okresie. Z tego względu w RODO

przewidziano możliwość sukcesywnego dokonywania zgłoszenia. Możliwość ta będzie prawdopodobnie wykorzystywana w przypadku bardziej złożonych naruszeń, takich jak niektóre rodzaje cyberincydentów, w przypadku których pełne ustalenie charakteru naruszenia oraz skali naruszenia ochrony danych osobowych może wiązać się np. z koniecznością przeprowadzenia dogłębnego dochodzenia kryminalistycznego. Z tego względu w wielu przypadkach administrator będzie zobowiązany do przeprowadzenia szerzej zakrojonych postępowań i podjęcia działań następczych w momencie uzyskania dodatkowych informacji na późniejszym etapie. Taką sytuację uznaje się za dopuszczalną, o ile administrator wyjaśni przyczyny opóźnienia zgodnie z art. 33 ust. 1. Grupa Robocza Art. 29 zaleca, aby w momencie, w którym administrator po raz pierwszy zgłasza dane naruszenie organowi nadzorczemu, poinformował również ten organ o tym, że nie dysponuje jeszcze wszystkimi wymaganymi danymi i że przekaże bardziej szczegółowe informacji na późniejszym etapie. Organ nadzorczy powinien uzgodnić z administratorem sposób i termin przekazania tych dodatkowych informacji. Nie uniemożliwia to administratorowi udzielania dodatkowych informacji na dowolnym innym etapie w przypadku, gdy uzyska wiedzę o dalszych istotnych okolicznościach faktycznych związanych z naruszeniem, która powinna zostać przekazana organowi nadzorczemu.

Wymóg zgłaszania naruszeń ustanowiono przede wszystkim, aby zachęcić administratorów do szybkiego reagowania na naruszenia, ograniczania ich wpływu oraz – w miarę możliwości – odzyskiwania danych osobowych, których bezpieczeństwo zostało naruszone, a także zasięgania opinii organu nadzorczego w tym zakresie. Zgłoszenie naruszenia organowi nadzorczemu w ciągu pierwszych 72 godzin od jego wystąpienia może umożliwić administratorowi zagwarantowanie podjęcia prawidłowych decyzji w kwestii tego, czy w danym przypadku należy zawiadomić osoby fizyczne o wystąpieniu naruszenia.

Celem zgłoszenia naruszenia organowi nadzorczemu nie jest jednak wyłącznie uzyskanie wskazówek w kwestii tego, czy o jego wystąpieniu należy zawiadomić osoby fizyczne, na które wywiera ono wpływ. W niektórych przypadkach administrator – opierając się na charakterze naruszenia i powadze związanego z nim ryzyka – będzie mógł jednoznacznie stwierdzić, że osoby fizyczne, na które dane naruszenie wywiera wpływ, muszą zostać niezwłocznie zawiadomione o jego wystąpieniu. Na przykład w sytuacji bezpośredniego zagrożenia kradzieżą tożsamości lub ujawnieniem szczególnych kategorii danych osobowych[26] w internecie administrator powinien bez zbędnej zwłoki podjąć działania mające na celu ograniczenie skali naruszenia i zawiadomienie osób fizycznych, na które wywiera ono wpływ, o jego wystąpieniu (zob. sekcja III). W wyjątkowych okolicznościach administrator może zawiadomić osoby fizyczne o wystąpieniu naruszenia przed zgłoszeniem naruszenia organowi nadzorczemu. Ogólniej rzecz biorąc, zgłoszenie naruszenia organowi nadzorczemu nie może stanowić usprawiedliwienia dla niewywiązania się z obowiązku zawiadomienia osoby, której dane dotyczą, o wystąpieniu naruszenia w przypadkach, w których jest to konieczne.

Należy również podkreślić, że po dokonaniu początkowego zgłoszenia administrator może przekazywać organowi nadzorczemu bardziej aktualne informacje, jeżeli w toku postępowania przeprowadzonego po stwierdzeniu naruszenia ujawnione zostaną dowody świadczące o tym, że incydent bezpieczeństwa został zneutralizowany i że w rzeczywistości nie doszło do żadnego naruszenia. Takie informacje mogą następnie zostać wykorzystane jako uzupełnienie informacji, które zostały już przekazane organowi nadzorczemu, a sam incydent powinien zostać zarejestrowany jako niewiążący się z naruszeniem. Nie przewidziano żadnych sankcji z tytułu zgłaszania incydentów, co do których w ostatecznym rozrachunku okazało się, że nie wiązały się z naruszeniem.

Przykład

Administrator zgłasza organowi nadzorczemu utratę pamięci USB zawierającej kopię danych osobowych niektórych z jego klientów w terminie 72 godzin od wykrycia wystąpienia naruszenia. Pamięć USB zostaje następnie odnaleziona wśród innych dokumentów przechowywanych w pomieszczeniach administratora i odzyskana. Administrator przekazuje stosowne informacje w tym zakresie organowi nadzorczemu i występuje o zmianę treści zgłoszenia.

Należy przy tym podkreślić, że podejście bazujące na sukcesywnym zgłaszaniu naruszeń jest już stosowane w kontekście zobowiązań ustanowionych w dyrektywie 2002/58/WE i rozporządzeniu nr 611/2013 oraz w kontekście innych samodzielnie zgłaszanych incydentów.

3. Zgłoszenia dokonane z opóźnieniem

W art. 33 ust. 1 wyraźnie stwierdzono, że do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia. Na mocy tego przepisu – w połączeniu z koncepcją sukcesywnego dokonywania zgłoszenia – uznaje się, że administrator może nie zawsze być w stanie zgłosić naruszenie w wyznaczonym terminie oraz że dokonanie zgłoszenia z opóźnieniem może być w niektórych przypadkach dopuszczalne.

Taka sytuacja może wystąpić np. wówczas, gdy administrator będzie musiał w krótkim czasie stawić czoła szeregowi podobnych naruszeń dotyczących poufności danych wywierających taki sam wpływ na dużą liczbę osób, których dane dotyczą. Administrator może stwierdzić wystąpienie naruszenia i – na początkowym etapie postępowania, przed jego zgłoszeniem – wykryć kolejne podobne naruszenia wynikające z różnych przyczyn. W zależności od okoliczności danej sprawy ustalenie skali naruszeń może zająć administratorowi pewną ilość czasu, dlatego też zamiast zgłaszać poszczególne naruszenia indywidualnie, administrator może zgromadzić je w ramach jednego większego zgłoszenia uwzględniającego szereg bardzo podobnych naruszeń, które potencjalnie mogą wynikać z różnych przyczyn. W rezultacie naruszenia mogą zostać zgłoszone organowi nadzorczemu z opóźnieniem większym niż 72 godziny od momentu, w którym administrator po raz pierwszy stwierdził ich wystąpienie.

Ściśle rzecz biorąc, każde pojedyncze naruszenie stanowi incydent, który należy zgłosić. Aby jednak uniknąć nadmiernego obciążania administratorów, zapewniono im możliwość „zbiorczego" zgłoszenia wszystkich takich naruszeń, o ile dotyczą one tego samego rodzaju danych osobowych, których ochrona została naruszona w taki sam sposób, i o ile doszło do nich w stosunkowo krótkim odstępie czasu. Jeżeli w danym przypadku doszło do szeregu naruszeń dotyczących różnych rodzajów danych osobowych, których ochrona została naruszona w różny sposób, zgłoszenia należy dokonać w standardowym trybie, zgłaszając każde naruszenie zgodnie z przepisami art. 33.

Choć w niektórych przypadkach w RODO dopuszcza się możliwość dokonywania zgłoszeń z opóźnieniem, takie sytuacje należy traktować jako sytuacje nadzwyczajne. W tym względzie warto podkreślić, że zgłoszeń zbiorczych można również dokonywać w celu zgłoszenia szeregu podobnych naruszeń w wyznaczonym terminie 72 godzin.

C. Naruszenia o charakterze transgranicznym i naruszenia w jednostkach organizacyjnych spoza UE

1. Naruszenia o charakterze transgranicznym

W przypadku, w którym dochodzi do transgranicznego przetwarzania[27] danych osobowych, naruszenie może wywierać wpływ na osoby, których dane dotyczą, w więcej niż jednym państwie członkowskim. W art. 33 ust. 1 wyraźnie stwierdzono, że w przypadku wystąpienia naruszenia,

[26] Zob. art. 9.

[27] Zob. art. 4 pkt 23.

administrator powinien zgłosić je organowi nadzorczemu właściwemu zgodnie z art. 55 RODO[28]. Art. 55 ust. 1 stanowi, że:

> „Każdy organ nadzorczy jest właściwy do wypełniania zadań i wykonywania uprawnień powierzonych mu zgodnie z niniejszym rozporządzeniem na terytorium swojego państwa członkowskiego".

Art. 56 ust. 1 stanowi jednak, że:

> „Bez uszczerbku dla art. 55 organ nadzorczy głównej lub pojedynczej jednostki organizacyjnej administratora lub podmiotu przetwarzającego jest właściwy do podejmowania działań jako wiodący organ nadzorczy – zgodnie z procedurą przewidzianą w art. 60 – względem transgranicznego przetwarzania dokonywanego przez tego administratora lub ten podmiot przetwarzający".

Ponadto art. 56 ust. 6 stanowi, że:

> „Administrator lub podmiot przetwarzający komunikują się w sprawie dokonywanego przez nich transgranicznego przetwarzania jedynie z wiodącym organem nadzorczym".

Oznacza to, że administrator będzie zobowiązany do zgłoszenia naruszenia wiodącemu organowi nadzorczemu za każdym razem, gdy w kontekście transgranicznego przetwarzania dojdzie do naruszenia wymagającego zgłoszenia[29]. Dlatego też przy sporządzaniu swojego planu reagowania na naruszenia administrator musi ustalić, który organ nadzorczy jest wiodącym organem nadzorczym, któremu należy zgłosić naruszenie[30]. Dzięki temu administrator będzie mógł szybko reagować na pojawiające się naruszenia i wywiązywać się z zobowiązań spoczywających na nim zgodnie z art. 33. W tym kontekście należy wyjaśnić, że naruszenie wiążące się z transgranicznym przetwarzaniem należy zgłosić wiodącemu organowi nadzorczemu, którego siedziba niekoniecznie musi znajdować się w tym samym miejscu co miejsce, w którym znajdują się osoby, których dane dotyczą, lub co miejsce, w którym doszło do naruszenia. Zgłaszając naruszenie wiodącemu organowi nadzorczemu, administrator powinien – w stosownych przypadkach – określić, czy naruszenie dotyczy jednostek organizacyjnych znajdujących się w innych państwach członkowskich, oraz wskazać państwa członkowskie, w których dane naruszenie może potencjalnie wywrzeć wpływ na osoby, których dane dotyczą. Jeżeli administrator ma jakiekolwiek wątpliwości co do tożsamości wiodącego organu nadzorczego, powinien przynajmniej zgłosić naruszenie lokalnemu organowi nadzorczemu w miejscu, w którym doszło do naruszenia.

2. Naruszenia w jednostkach organizacyjnych spoza UE

Art. 3 dotyczy terytorialnego zakresu stosowania RODO, uwzględniając przypadki, w których przepisy RODO mają zastosowanie do przetwarzania danych osobowych przez administratora lub

[28] Zob. również motyw 122.

[29] Zob. wytyczne Grupy Roboczej Art. 29 dotyczące ustalania wiodącego organu nadzorczego właściwego dla administratora lub podmiotu przetwarzającego dostępne pod adresem: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611235

[30] Z wykazem danych kontaktowych wszystkich krajowych organów ochrony danych w Europie można zapoznać się pod adresem: http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm

podmiot przetwarzający niemających jednostek organizacyjnych w UE. W szczególności art. 3 ust. 2 stanowi, że[31]:

> „Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych osób, których dane dotyczą, przebywających w Unii przez administratora lub podmiot przetwarzający niemających jednostek organizacyjnych w Unii, jeżeli czynności przetwarzania wiążą się z:
>
> a) oferowaniem towarów lub usług takim osobom, których dane dotyczą, w Unii – niezależnie od tego, czy wymaga się od tych osób zapłaty; lub
>
> b) monitorowaniem ich zachowania, o ile do zachowania tego dochodzi w Unii".

W tym kontekście za istotne należy również uznać przepisy art. 3 ust. 3, który stanowi, że[32]:

> „Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych przez administratora niemającego jednostki organizacyjnej w Unii, ale posiadającego jednostkę organizacyjną w miejscu, w którym na mocy prawa międzynarodowego publicznego ma zastosowanie prawo państwa członkowskiego".

A zatem w przypadku, gdy naruszenie odnotuje administrator niemający jednostki organizacyjnej w UE, który podlega przepisom art. 3 ust. 2 lub 3, na administratorze tym wciąż spoczywają obowiązki zgłaszania określone w art. 33 i 34. W art. 27 ustanowiono wymóg zobowiązujący administratora (i podmiot przetwarzający) do wyznaczenia przedstawiciela w UE w przypadku, gdy zastosowanie ma art. 3 ust. 2. W takich przypadkach Grupa Robocza Art. 29 zaleca, aby zgłoszenia były kierowane do organu nadzorczego w państwie członkowskim, w którym przedstawiciel administratora w UE ma jednostkę organizacyjną[33]. Podobnie w przypadku gdy podmiot przetwarzający podlega przepisom art. 3 ust. 2, spoczywają na nim obowiązki dotyczące podmiotów przetwarzających, a w szczególności obowiązek zgłaszania naruszenia administratorowi na podstawie art. 33 ust. 2.

D. Sytuacje, w których zgłaszanie nie jest konieczne

W art. 33 ust. 1 wyraźnie stwierdzono, że nie ma obowiązku zgłaszania organowi nadzorczemu naruszeń, co do których „jest mało prawdopodobne, by [...] skutkował[y] ryzykiem naruszenia praw lub wolności osób fizycznych". Przykładem może być sytuacja, w której dane osobowe już są publicznie dostępne i ujawnienie takich danych nie wiąże się z prawdopodobnym ryzykiem dla danej osoby fizycznej. Jest to sprzeczne z istniejącymi wymogami powiadamiania o naruszeniu określonymi w dyrektywie 2009/136/WE, które spoczywają na dostawcach publicznie dostępnych usług łączności elektronicznej, zgodnie z którymi wszelkie istotne naruszenia należy zgłaszać właściwemu organowi.

W swojej opinii 03/2014 na temat powiadamiania o przypadkach naruszenia[34] Grupa Robocza Art. 29 wyjaśniła, że naruszenie poufności danych osobowych, które zaszyfrowano przy użyciu najnowocześniejszego algorytmu, nadal stanowi naruszenie danych osobowych i musi zostać

[31] Zob. również motywy 23 i 24.

[32] Zob. również motyw 25.

[33] Zob. motyw 80 i art. 27.

[34] Grupa Robocza Art. 29, opinia 03/2014 na temat powiadamiania o przypadkach naruszenia: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp213_pl.pdf

zgłoszone. Jeżeli jednak nie dojdzie do naruszenia poufności klucza – tj. jeżeli klucz nie został złamany w wyniku naruszenia bezpieczeństwa oraz został wygenerowany w sposób, który uniemożliwia osobie nieupoważnionej poznanie go za pomocą dostępnych technologicznie środków – to dane zasadniczo pozostają nieczytelne. Nie jest więc prawdopodobne, aby takie naruszenie wywarło niekorzystny wpływ na osoby, których dane dotyczą, a zatem nie zachodzi konieczność powiadomienia o nim takich osób[35]. Nawet jeżeli dane są zaszyfrowane, ich utrata lub zmiana może jednak wywrzeć niekorzystny wpływ na osoby, których dane dotyczą, jeżeli administrator danych nie posiada odpowiednich kopii zapasowych. W takim przypadku należy powiadomić osoby, których dane dotyczą, nawet jeżeli same dane odpowiednio zaszyfrowano.

Grupa Robocza Art. 29 wyjaśniła również, że taka sama sytuacja miałaby miejsce, gdyby w stosunku do danych osobowych, takich jak hasła, zastosowano bezpieczną funkcję skrótu i ciągu zaburzającego, dane zostały zastąpione wartością klucza haszującego, obliczoną za pomocą najnowocześniejszej kryptograficznej funkcji haszującej z kluczem tajnym, klucz użyty do haszowania tych danych nie został złamany w wyniku naruszenia bezpieczeństwa, oraz został wygenerowany w sposób, który uniemożliwia osobie nieupoważnionej poznanie go za pomocą dostępnych technologicznie środków.

A zatem, jeżeli zapewniono, aby dane osobowe były zasadniczo nieczytelne dla osób nieupoważnionych, oraz jeżeli dane są kopią lub istnieje kopia bezpieczeństwa, nie ma potrzeby zgłaszania organowi nadzorczemu naruszenia dotyczącego poufności danych związanego z odpowiednio zaszyfrowanymi danymi osobistymi. Wynika to z niskiego prawdopodobieństwa, że takie naruszenie stworzy ryzyko naruszenia praw i wolności osób fizycznych. Oznacza to oczywiście, że nie ma również konieczności powiadamiania danej osoby fizycznej, ponieważ ryzyko prawdopodobnie nie jest wysokie. Warto jednak pamiętać, że choć początkowo zgłoszenie może nie być wymagane ze względu na fakt, iż prawdopodobieństwo wystąpienia ryzyka naruszenia praw i wolności osób fizycznych jest niskie, z czasem sytuacja może się zmienić i może wystąpić konieczność przeprowadzenia kolejnej oceny ryzyka. Przykładowo konieczność zgłoszenia może występować także w sytuacji, gdy w późniejszym czasie stwierdzono, że klucz został złamany, lub wykryto lukę w oprogramowaniu szyfrującym.

Należy również podkreślić, że wystąpienie naruszenia w sytuacji, w której nie istnieje kopia bezpieczeństwa zaszyfrowanych danych osobowych, oznacza, iż miało miejsce naruszenie dotyczące dostępności danych, które może stwarzać ryzyko dla osób fizycznych i w związku z tym może wymagać zgłoszenia. Sytuacja jest podobna w przypadku wystąpienia naruszenia związanego z utratą zaszyfrowanych danych – nawet jeżeli istnieje kopia bezpieczeństwa danych osobowych – takie naruszenie może również wymagać zgłoszenia w zależności od tego, ile czasu zajęło przywracanie danych z kopii zapasowej, oraz od tego, jak brak dostępności wpłynął na osoby fizyczne. Zgodnie z art. 32 ust. 1 lit. c) istotnym czynnikiem gwarantującym bezpieczeństwo jest „zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego".

Przykład

Przykładem naruszenia, które nie wymagałoby zgłoszenia organowi nadzorczemu, byłaby utrata bezpiecznie zaszyfrowanego urządzenia mobilnego, z którego korzystają administrator i jego pracownicy. Zakładając, że klucz kryptograficzny jest bezpiecznie przechowywany przez administratora i nie jest to jedyna kopia danych osobowych, dane osobowe będą niedostępne dla atakującego. Oznacza to, że przedmiotowe naruszenie najprawdopodobniej nie będzie wiązało się z ryzykiem naruszenia praw i wolności osób, których te dane dotyczą. Jeżeli później okaże się, że klucz kryptograficzny został złamany lub oprogramowanie lub algorytm szyfrujący ma słabe punkty, poziom ryzyka naruszenia praw i wolności osób fizycznych zmieni się i wówczas zgłoszenie może stać się konieczne.

[35] Zob. również art. 4 ust. 1 i 2 rozporządzenia nr 611/2013.

Jeżeli jednak administrator nie powiadomi organu nadzorczego w sytuacji, w której dane w rzeczywistości nie zostały bezpiecznie zaszyfrowane, wówczas ma miejsce niewywiązanie się z zobowiązań wynikających z art. 33. Dokonując wyboru oprogramowania szyfrującego, administratorzy powinni zatem dokładnie zastanowić się nad jakością i odpowiednim wdrożeniem oferowanej metody szyfrowania, dowiedzieć się, jaki poziom ochrony faktycznie ona zapewnia, oraz czy jest adekwatna do poziomu istniejącego ryzyka. Administratorzy powinni również być zaznajomieni ze szczegółami funkcjonowania wykorzystywanego przez nich produktu szyfrującego. Na przykład urządzenie może być szyfrowane po wyłączeniu, ale nie wtedy, gdy znajduje się w trybie uśpienia. Niektóre produkty wykorzystujące szyfrowanie mogą posiadać „domyślne klucze", które każdy klient musi zmienić, aby szyfrowanie było skuteczne. Chociaż eksperci ds. bezpieczeństwa mogą obecnie uznawać daną metodę szyfrowania za odpowiednią, może ona się za kilka lat stać przestarzała, co stworzy wątpliwości, czy szyfrowanie danych zapewniane przez ten produkt będzie wystarczające i czy będzie zapewniało właściwy poziom ochrony.

III. Art. 34 – Zawiadamianie osoby, której dane dotyczą

A. Zawiadamianie osób fizycznych

W niektórych przypadkach administrator musi nie tylko zgłosić naruszenie organowi nadzorczemu, ale również powiadomić o nim osoby fizyczne, na które to naruszenie wywiera wpływ.

Art. 34 ust. 1 stanowi, że:

„Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu".

Administratorzy powinni pamiętać, że zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu jest obowiązkowe, chyba że jest mało prawdopodobne, by skutkowało ono ryzykiem naruszenia praw i wolności osób fizycznych. Ponadto jeżeli istnieje prawdopodobieństwo, że naruszenie ochrony danych osobowych spowoduje wysokie ryzyko naruszenia praw i wolności osób fizycznych, należy poinformować o nim również osoby fizyczne. A zatem poziom zagrożenia skutkujący powstaniem obowiązku przekazania osobom fizycznym informacji o naruszeniu jest wyższy niż w przypadku zgłaszania naruszenia organom nadzorczym, dzięki czemu nie ma obowiązku zgłaszania osobom fizycznym wszystkich naruszeń, co pozwala ochronić je przed nadmiarem niepotrzebnych powiadomień.

RODO stanowi, że osoby fizyczne należy poinformować o naruszeniu „bez zbędnej zwłoki" – tj. najszybciej, jak to możliwe. Zawiadomienie osób fizycznych ma na celu przede wszystkim dostarczenie im szczegółowych informacji na temat działań zapobiegawczych, które powinny podjąć[36]. Jak wspomniano powyżej, w zależności od charakteru naruszenia i powstałego ryzyka, szybkie zawiadomienie pozwoli osobom fizycznym podjąć działania, aby uchronić się przed wszelkimi negatywnymi skutkami naruszenia.

[36] Zob. również motyw 86.

W załączniku B do niniejszych wytycznych przedstawiono niewyczerpujący wykaz przykładowych sytuacji, w których istnieje duże prawdopodobieństwo, że naruszenie stworzy wysokie ryzyko dla osób fizycznych, a co za tym idzie przypadków, w których administrator musi zgłosić wystąpienie naruszenia osobom, na które ma ono wpływ.

B. Informacje, których należy udzielić

W odniesieniu do zawiadamiania osób fizycznych art. 34 ust. 2 stanowi, że:

„Zawiadomienie, o którym mowa w ust. 1 niniejszego artykułu, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w art. 33 ust. 3 lit. b), c) i d)".

Zgodnie z tym przepisem administrator musi udzielić co najmniej następujących informacji:

- opis charakteru naruszenia;
- imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego;
- opis możliwych konsekwencji naruszenia; oraz
- opis środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

Jednym z przykładów środków zastosowanych w celu zaradzenia naruszeniu i zminimalizowania jego ewentualnych negatywnych skutków może być deklaracja administratora, że po zgłoszeniu naruszenia właściwemu organowi nadzorczemu administrator uzyskał zalecenie dotyczące zarządzania naruszeniem i ograniczenia jego wpływu. Administrator powinien również – w stosownych przypadkach – przekazać osobom fizycznym szczegółowe zalecenia na temat sposobów ochrony przed potencjalnymi niekorzystnymi skutkami naruszenia – takich jak zmiana haseł – jeżeli ich dane uwierzytelniające zostały ujawnione. Również w tym wypadku administrator może podjąć decyzję o przekazaniu większej ilości informacji, niż jest to wymagane.

C. Kontakt z osobami fizycznymi

Co do zasady osoby, których dane dotyczą, należy zawiadomić o naruszeniu bezpośrednio, chyba że takie działanie wymagałoby niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób (art. 34 ust. 3 lit. c)).

Osoby, których dane dotyczą, należy zawiadamiać o naruszeniu za pomocą specjalnie do tego przeznaczonych wiadomości i nie należy tych wiadomości przesyłać wraz z innymi informacjami, takimi jak regularne aktualizacje, biuletyny lub standardowe wiadomości. Dzięki temu zawiadomienie o naruszeniu będzie jasne i przejrzyste.

Do przykładów przejrzystych metod zawiadamiania należą komunikacja bezpośrednia (np. wiadomości e-mail, SMS, wiadomości bezpośrednie), rzucające się w oczy bannery lub powiadomienia na stronach internetowych, komunikacja pocztowa oraz rzucające się w oczy reklamy w mediach drukowanych. Powiadomienie, które jest tylko częścią komunikatu prasowego lub zostało zamieszczone na blogu przedsiębiorstwa, nie byłoby skuteczną metodą zawiadomienia osób fizycznych o naruszeniu. Zgodnie z zaleceniami Grupy Roboczej Art. 29 administratorzy powinni wybierać metody pozwalające zapewnić jak największą szansę właściwego przekazania informacji wszystkim osobom fizycznym, na które to naruszenie wywiera wpływ. W niektórych okolicznościach może to oznaczać, że administrator wykorzysta szereg metod komunikacji, a nie tylko jeden kanał kontaktowy.

Może zdarzyć się, że administratorzy będą również musieli zapewnić dostępność zawiadomienia w odpowiednich formatach alternatywnych i stosownych językach, aby zapewnić osobom fizycznym możliwość zrozumienia przedstawionych im informacji. Na przykład do zawiadomienia osoby fizycznej o naruszeniu właściwy będzie zazwyczaj język wykorzystywany we wcześniejszych zwykłych relacjach gospodarczych z odbiorcą. Jednak jeżeli naruszenie ma wpływ na osoby, z którymi administrator nie miał wcześniej kontaktu, lub w szczególności na osoby zamieszkujące w państwie członkowskim lub państwie trzecim innym niż państwo, w którym administrator posiada jednostkę organizacyjną, dopuszczalne może być użycie w zawiadomieniu miejscowego języka urzędowego, uwzględniając przy tym potrzebne zasoby. Najważniejsze, aby osoby, których dane dotyczą, zrozumiały charakter naruszenia i wiedziały, co muszą zrobić, aby się zabezpieczyć.

Administratorzy mają największe kompetencje do określenia kanału kontaktowego, który byłby najwłaściwszy do zawiadomienia osób fizycznych o naruszeniu, w szczególności jeżeli regularnie wchodzą w interakcję ze swoimi klientami. Jest jednak oczywiste, że administrator powinien uważać, aby nie wykorzystywać kanału kontaktowego, który w wyniku naruszenia przestał być bezpieczny, ponieważ kanał ten mogą wykorzystać również atakujący podszywający się pod administratora.

Jednocześnie w motywie 86 wyjaśniono, że:

„Informacje należy przekazywać osobom, których dane dotyczą, tak szybko, jak jest to rozsądnie możliwe, w ścisłej współpracy z organem nadzorczym, z poszanowaniem wskazówek przekazanych przez ten organ lub inne odpowiednie organy, takie jak organy ścigania. Na przykład potrzeba zminimalizowania bezpośredniego ryzyka wystąpienia szkody będzie wymagać niezwłocznego poinformowania osób, których dane dotyczą, natomiast wdrożenie odpowiednich środków przeciwko takim samym lub podobnym naruszeniom ochrony danych może uzasadniać późniejsze poinformowanie".

Kontakt i konsultacje z organem nadzorczym pozwolą administratorom uzyskać nie tylko zalecenia na temat powiadamiania osób, których dane dotyczą, o naruszeniu zgodnie z art. 34, ale również na temat stosownych wiadomości, które należy wysłać do osób fizycznych, oraz najwłaściwszego sposobu skontaktowania się z nimi.

Kwestii tej dotyczy zalecenie zawarte w motywie 88, które stanowi, że w zawiadomieniu o naruszeniu „należy [...] uwzględnić prawnie uzasadnione interesy organów ścigania, jeżeli przedwczesne ujawnienie mogłoby niepotrzebnie utrudnić badanie okoliczności naruszenia ochrony danych osobowych". Może to oznaczać, że w pewnych okolicznościach, gdy jest to uzasadnione, oraz zgodnie z zaleceniami organów ścigania administrator może opóźnić wysłanie zawiadomienia o naruszeniu do osób fizycznych, na które wywiera ono wpływ, do momentu, w którym takie zawiadomienie nie zaszkodzi takim postępowaniom. Osoby, których dane dotyczą, należy jednak wciąż natychmiast poinformować po upływie tego okresu.

Jeżeli administrator nie jest w stanie zawiadomić danej osoby fizycznej o naruszeniu, ponieważ przechowywane dane są niewystarczające do skontaktowania się z tą osobą, w takim szczególnym przypadku administrator powinien ją poinformować tak szybko, jak jest to rozsądnie wykonalne (np. jeżeli osoba fizyczna skorzysta z przewidzianego w art. 15 prawa do uzyskania dostępu do swoich danych osobowych i dostarczy administratorowi dodatkowe informacje wymagane do skontaktowania się z nią).

D. Sytuacje, w których zawiadomienie nie jest konieczne

W art. 34 ust. 3 określono trzy sytuacje, w których nie ma konieczności zawiadomienia osób fizycznych w przypadku wystąpienia naruszenia. Sytuacje te są następujące:

- administrator zastosował przed wystąpieniem naruszenia odpowiednie techniczne i organizacyjne środki w celu ochrony danych osobowych, w szczególności środki

uniemożliwiające odczyt danych osobom, które nie są uprawnione do dostępu do tych danych. Może to na przykład obejmować zabezpieczenie danych osobowych za pomocą najnowocześniejszego szyfrowania lub tokenizacji;

- natychmiast po wystąpieniu naruszenia administrator podjął działania w celu wyeliminowania prawdopodobieństwa powstania wysokiego ryzyka naruszenia praw lub wolności osoby fizycznej. Na przykład w niektórych sytuacjach administrator mógł natychmiast zidentyfikować osobę fizyczną, która uzyskała dostęp do danych osobowych, i podjąć wobec niej działania, zanim mogła ona w jakikolwiek sposób wykorzystać te dane. Mimo to należy odpowiednio uwzględnić możliwe skutki każdego naruszenia poufności, również w tym wypadku biorąc pod uwagę charakter przedmiotowych danych;
- skontaktowanie się z danymi osobami fizycznymi wymagałoby niewspółmiernie dużego wysiłku[37], na przykład ponieważ w wyniku naruszenia utracono ich dane kontaktowe albo dane te nigdy nie były znane. Na przykład archiwum urzędu statystycznego uległo zalaniu, a dokumenty zawierające dane osobowe przechowywano tylko w formie papierowej. W takim przypadku administrator musi wydać publiczny komunikat lub zastosować podobny środek, za pomocą którego osoby fizyczne zostaną poinformowane w równie skuteczny sposób. Jeżeli wykonanie tego działania wymagałoby niewspółmiernie dużego wysiłku, można również przewidzieć uzgodnienia techniczne, dzięki którym informacje na temat naruszenia będą dostępne na żądanie, co może okazać się przydatne dla osób, na które naruszenie mogło wywrzeć wpływ, lecz z którymi administrator nie mógł się w inny sposób skontaktować.

Zgodnie z zasadą rozliczalności administratorzy powinni być w stanie wykazać przed organem nadzorczym, że spełniają co najmniej jeden z tych warunków[38]. Warto pamiętać, że choć początkowo zgłoszenie może nie być wymagane ze względu na fakt, iż prawdopodobieństwo wystąpienia ryzyka naruszenia praw i wolności osób fizycznych jest niskie, z czasem sytuacja może się zmienić i może wystąpić konieczność przeprowadzenia kolejnej oceny ryzyka.

Jeżeli administrator zdecyduje się nie zawiadamiać osoby fizycznej o naruszeniu, w art. 34 ust. 4 wyjaśniono, że organ nadzorczy może od niego tego zażądać, jeżeli jego zdaniem naruszenie może powodować wysokie ryzyko dla osób fizycznych. Ewentualnie może stwierdzić, że spełnione zostały warunki, o których mowa w art. 34 ust. 3, i w takim przypadku zawiadomienie osób fizycznych nie jest konieczne. Jeżeli organ nadzorczy stwierdzi, że decyzja o niezawiadamianiu osób, których dane dotyczą, nie jest odpowiednio uzasadniona, może rozważyć wykorzystanie swoich uprawnień i nałożenie sankcji.

IV. Ocena ryzyka i wysokiego ryzyka

A. Ryzyko jako powód zgłoszenia

Mimo że w RODO wprowadzono obowiązek zgłaszania naruszenia, nie jest ono wymagane we wszystkich sytuacjach:

[37] Zob. wytyczne Grupy Roboczej Art. 29 w sprawie przejrzystości, w których zajęto się kwestią niewspółmiernie dużego wysiłku, dostępne pod adresem: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850

[38] Zob. art. 5 ust. 2.

- zgłoszenie naruszenia właściwemu organowi nadzorczemu jest obowiązkowe, chyba że dane naruszenie najprawdopodobniej nie będzie wiązało się z ryzykiem naruszenia praw i wolności osób fizycznych;
- osobę fizyczną zawiadamia się o naruszeniu jedynie wówczas, gdy naruszenie może powodować wysokie ryzyko naruszenia praw i wolności tych osób.

Oznacza to, że natychmiast po stwierdzeniu naruszenia administrator musi nie tylko dążyć do ograniczenia negatywnych skutków incydentu, lecz również ocenić ryzyko, które może powstać w wyniku tego naruszenia. Wynika to z dwóch ważnych przyczyn: po pierwsze, znajomość prawdopodobieństwa i potencjalnej dotkliwości wpływu na osoby fizyczne pomoże administratorowi w podjęciu skutecznych działań pozwalających zapanować nad skutkami naruszenia i je zminimalizować; po drugie, pomoże administratorowi stwierdzić, czy zgłoszenie naruszenia organowi nadzorczemu oraz – w stosownych przypadkach – osobom, których dotyczy naruszenie, jest konieczne.

Jak wyjaśniono powyżej, zgłoszenie naruszenia jest obowiązkowe, chyba że jest mało prawdopodobne, by skutkowało ono ryzykiem naruszenia praw i wolności osób fizycznych, a to, czy o naruszeniu należy zawiadomić osoby, których dane dotyczą, zależy przede wszystkim od tego, czy naruszenie może powodować *wysokie* ryzyko naruszenia praw i wolności osób fizycznych. Ryzyko to istnieje w przypadku, gdy naruszenie może prowadzić do uszczerbku fizycznego lub szkód majątkowych lub niemajątkowych dla osób, których dane zostały naruszone. Przykłady takich szkód obejmują dyskryminację, kradzież lub sfałszowanie tożsamości, straty finansowe i naruszenie dobrego imienia. Jeżeli naruszenie obejmuje dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, wyznanie lub przekonania światopoglądowe, lub przynależność do związków zawodowych oraz jeżeli przetwarzane są dane genetyczne, dane dotyczące zdrowia lub seksualności lub dane dotyczące wyroków skazujących i naruszeń prawa lub związanych z tym środków bezpieczeństwa – należy uznać, że taka szkoda prawdopodobnie nastąpi[39].

B. Czynniki, które należy uwzględnić podczas oceny ryzyka

Zgodnie z zaleceniami zawartymi w motywach 75 i 76 RODO podczas oceny ryzyka zasadniczo należy wziąć pod uwagę zarówno prawdopodobieństwo, jak i powagę ryzyka naruszenia praw lub wolności osób, których dane dotyczą. Stwierdzono również, że ryzyko naruszenia należy oszacować na podstawie obiektywnej oceny.

Należy podkreślić, że podczas oceny ryzyka naruszenia praw i wolności osób fizycznych powstałego w wyniku wystąpienia naruszenia kładzie się nacisk na inne kwestie, niż kwestie dotyczące ryzyka uwzględniane w ocenie skutków dla ochrony danych[40]. W ocenie skutków dla ochrony danych bierze się pod uwagę zarówno ryzyko dla planowego przetwarzania danych, jak i ryzyko powstałe w przypadku wystąpienia naruszenia. Badając możliwe naruszenie, rozpatruje się w ujęciu ogólnym prawdopodobieństwo jego wystąpienia oraz szkody dla osób, których dane dotyczą, jakie mogą z niego wyniknąć; innymi słowy, jest to ocena wydarzenia hipotetycznego. W przypadku faktycznego naruszenia wydarzenie już nastąpiło, więc nacisk kładzie się w całości na powstałe ryzyko, że naruszenie będzie skutkowało wpływem na osoby fizyczne.

Przykład

[39] Zob. motywy 75 i 85.

[40] Zob. wytyczne Grupy Roboczej na temat oceny skutków dla ochrony danych dostępne pod adresem: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

Z oceny skutków dla ochrony danych wynika, że rozważane wykorzystanie określonego oprogramowania zabezpieczającego do ochrony danych osobowych stanowi właściwy środek służący zapewnieniu stopnia bezpieczeństwa, który jest odpowiedni względem ryzyka dla osób fizycznych, jakie w innym przypadku wynikałoby z przetwarzania danych. Gdyby jednak w późniejszym czasie wykryto lukę w zabezpieczeniach, sytuacja ta wpłynęłaby na przydatność oprogramowania do ograniczenia ryzyka dla chronionych danych osobowych, a zatem oprogramowanie należałoby poddać ponownej ocenie w ramach trwającej oceny skutków dla ochrony danych.

Luka w oprogramowaniu zostaje później wykorzystana i następuje naruszenie. Administrator powinien przeprowadzić ocenę konkretnych okoliczności naruszenia, sprawdzić, których danych dotyczy naruszenie, a także oszacować potencjalny poziom wpływu na osoby fizyczne i prawdopodobieństwo wystąpienia tego ryzyka.

Oceniając ryzyko dla osób fizycznych będące wynikiem naruszenia, administrator powinien uwzględnić zatem konkretne okoliczności naruszenia, w tym wagę potencjalnego wpływu i prawdopodobieństwo jego wystąpienia. Grupa Robocza Art. 29 zaleca zatem, aby w trakcie oceny brano pod uwagę następujące kryteria[41]:

- Rodzaj naruszenia

Rodzaj stwierdzonego naruszenia może wpłynąć na poziom ryzyka dla osób fizycznych. Na przykład konsekwencje dla osoby fizycznej w przypadku naruszenia dotyczącego poufności danych, którego istotą jest ujawnienie informacji medycznych osobom nieupoważnionym, mogą być inne niż konsekwencje naruszenia polegającego na utracie informacji medycznych danej osoby, do których nie ma już dostępu.

- Charakter, wrażliwość i ilość danych osobowych

Kluczowym czynnikiem podczas oceniania ryzyka jest oczywiście rodzaj i wrażliwość danych osobowych, które zostały ujawnione w wyniku naruszenia. Zazwyczaj ryzyko powstania szkody dla osób, których dotyczy naruszenie, wzrasta wraz z wrażliwością danych, lecz należy wziąć pod uwagę również inne dane osobowe dotyczące tych osób, które mogą już być dostępne. Na przykład ujawnienie imienia i nazwiska oraz adresu danej osoby prawdopodobnie nie wyrządzi jej szkody w normalnej sytuacji. Jednak jeżeli imię i nazwisko oraz adres rodzica adopcyjnego zostaną ujawnione rodzicowi biologicznemu, może mieć to bardzo poważne konsekwencje zarówno dla rodzica adopcyjnego, jak i dziecka.

Naruszenia powiązane z danymi dotyczącymi zdrowia, dokumentami tożsamości lub danymi finansowymi takimi jak dane kart kredytowych mogą spowodować szkody, jeżeli występują pojedynczo, lecz jeżeli wystąpią łącznie, mogą zostać wykorzystane do kradzieży tożsamości. Zbiór różnych danych osobowych ma zazwyczaj bardziej wrażliwy charakter niż pojedynczy element danych osobowych.

Niektóre rodzaje danych osobowych mogą się na pierwszy rzut oka wydawać nieszkodliwe, ale należy dokładnie rozważyć, jakie informacje takie dane mogą ujawnić na temat osoby fizycznej, na którą naruszenie wywiera wpływ. Wykaz klientów regularnie odbierających dostawy może nie stanowić szczególnie wrażliwych danych, ale takie same dane na temat klientów, którzy poprosili o wstrzymanie dostaw na czas urlopu, byłyby dla przestępców przydatne.

Ponadto niewielka ilość bardzo wrażliwych danych osobowych może mieć znaczny wpływ na daną osobę fizyczną, a wiele różnych szczegółów może się ujawnić szerszy zakres informacji na temat tej osoby. Podobnie naruszenie, które ma wpływ na duże ilości danych osobowych dotyczące wielu osób, może wywołać skutki dla odpowiednio dużej liczby osób fizycznych.

- Łatwość identyfikacji osób fizycznych

Istotnym czynnikiem, który należy wziąć pod uwagę, jest łatwość, z jaką strona, która ma dostęp do ujawnionych danych osobowych, będzie w stanie zidentyfikować konkretne osoby fizyczne lub dopasować dane do innych informacji służących identyfikacji osób fizycznych. W zależności od okoliczności identyfikacja może być możliwa bezpośrednio w oparciu o dane osobowe, których dotyczy naruszenie, bez potrzeby gromadzenia dodatkowych informacji pozwalających określić tożsamość danej osoby lub dopasowanie danych osobowych do konkretnej osoby może być bardzo trudne, lecz wciąż wykonalne pod pewnymi warunkami. Identyfikacja może być pośrednio lub bezpośrednio możliwa w oparciu o ujawnione dane, ale może również zależeć od konkretnego kontekstu naruszenia i publicznej dostępności powiązanych danych osobowych. Może to mieć większe znaczenie w przypadku naruszeń dotyczących poufności i dostępności danych.

Jak stwierdzono powyżej, dane osobowe chronione za pomocą odpowiedniego poziomu szyfrowania będą nieczytelne dla osób nieupoważnionych, które nie posiadają klucza deszyfrującego. Ponadto odpowiednio wdrożona pseudonimizacja (zdefiniowana w art. 4 pkt 5 jako „przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej") również może zmniejszyć prawdopodobieństwo zidentyfikowania osób fizycznych w przypadku naruszenia. Jednak aby dane były nieczytelne, nie można polegać jedynie na technikach pseudonimizacji.

- Waga konsekwencji dla osób fizycznych

W zależności od charakteru danych osobowych, których dotyczy naruszenie – na przykład szczególnych kategorii danych osobowych – możliwe szkody, których mogą doznać osoby fizyczne, mogą być szczególnie poważne, zwłaszcza w przypadku gdy w wyniku naruszenia nastąpi kradzież lub sfałszowanie tożsamości, uszkodzenie ciała, cierpienie psychiczne, upokorzenie lub naruszenie dobrego imienia. Jeżeli naruszenie jest związane z danymi osobowymi dotyczącymi osób szczególnie narażonych, może to dla nich stwarzać większe ryzyko szkody.

To, czy administrator wie, że dane osobowe znajdują się w rękach osób, których zamiary są nieznane lub które mogą mieć złe intencje, może mieć znaczenie dla poziomu potencjalnego ryzyka. Może nastąpić naruszenie dotyczące poufności danych polegające na omyłkowym ujawnieniu danych osobowych stronie trzeciej, zgodnie z definicją w art. 4 pkt 10, lub innemu odbiorcy. Może to nastąpić na przykład w sytuacji, gdy dane osobowe zostaną przypadkowo wysłane do niewłaściwego działu organizacji lub do organizacji dostawców, z której usług powszechnie się korzysta. Administrator może wezwać odbiorcę do zwrotu albo bezpiecznego zniszczenia otrzymanych danych. W obu przypadkach – z uwagi na fakt, że administrator pozostaje z tymi podmiotami w stałych stosunkach i może znać stosowane przez nie procedury, ich historię i inne istotne szczegóły ich dotyczące – odbiorcę można uznać za „zaufanego". Innymi słowy, administrator może ufać odbiorcy na tyle, aby móc racjonalnie oczekiwać, że strona ta nie odczyta omyłkowo wysłanych danych lub nie uzyska do nich wglądu oraz że wypełni polecenie ich odesłania. Nawet jeżeli do danych uzyskano wgląd, administrator nadal może mieć zaufanie do odbiorcy, że nie podejmie on żadnych dalszych działań w kwestii tych danych oraz że niezwłocznie zwróci dane do administratora i będzie współpracować przy ich odzyskaniu. W takich przypadkach administrator może uwzględnić tę

[41] W art. 3 ust. 2 rozporządzenia nr 611/2013 przedstawiono wytyczne dotyczące czynników, które należy wziąć pod uwagę w związku ze zgłaszaniem naruszeń w sektorze usług łączności elektronicznej – mogą one okazać się przydatne w kontekście dokonywania zgłoszeń zgodnie z RODO. Zob. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:pl:PDF

kwestię w ocenie ryzyka przeprowadzanej w następstwie naruszenia – fakt, że odbiorca jest zaufany może spowodować, że skutki naruszenia nie będą poważne, ale nie znaczy to, że naruszenie nie miało miejsca. To z kolei może jednak wyeliminować prawdopodobieństwo wystąpienia ryzyka dla osób fizycznych, w wyniku czego nie będzie już potrzeby powiadomienia organu nadzorczego lub osób fizycznych, na które to naruszenie wywiera wpływ Również w tym wypadku wszystko będzie zależało od konkretnej sytuacji. Administrator wciąż jednak musi przechowywać informacje dotyczące naruszenia w ramach ogólnego obowiązku prowadzenia dokumentacji na temat naruszeń (zob. sekcja V poniżej).

Należy również zwrócić uwagę na to, jak trwałe są konsekwencje wobec osób fizycznych, gdyż wpływ może być postrzegany jako poważniejszy, jeżeli dotyczy długiego okresu.

- Cechy szczególne danej osoby fizycznej

Naruszenie może mieć wpływ na dane osobowe dotyczące dzieci lub innych osób szczególnie narażonych, w przypadku których w takiej sytuacji może występować większe ryzyko, że znajdą się w niebezpieczeństwie. Z daną osobą fizyczną mogą wiązać się również inne czynniki wpływające na wagę konsekwencji naruszenia, jakie mogą dla niej wyniknąć.

- Cechy szczególne administratora danych

Charakter i rola administratora oraz prowadzone przez niego działania mogą mieć wpływ na poziom ryzyka dla osób fizycznych wynikającego z naruszenia. Przykładowo w organizacji medycznej przetwarzane są szczególne kategorie danych osobowych, co oznacza, że w przypadku naruszenia tych danych osobowych osoby fizyczne są narażone na większe zagrożenie niż w przypadku, gdy naruszenie dotyczy listy adresowej czasopisma.

- Liczba osób fizycznych, na które naruszenie wywiera wpływ

Naruszenie może dotyczyć tylko jednej osoby, kilku osób lub kilku tysięcy osób – albo dużo większej ich liczby. Zazwyczaj potencjalny wpływ naruszenia wzrasta wraz z liczbą osób, których ono dotyczy. Jednak w zależności od charakteru danych osobowych oraz kontekstu, w którym zostały one ujawnione, naruszenie może mieć poważne konsekwencje nawet dla jednej osoby. Również w tym wypadku najważniejsze jest przeanalizowanie prawdopodobieństwa wystąpienia konsekwencji dla osób, na które naruszenie na wpływ, oraz tego, jak poważne będą te konsekwencje.

- Uwagi ogólne

W związku z tym podczas oceny ryzyka, które może powstać w wyniku naruszenia, administrator powinien łącznie uwzględnić wagę potencjalnego wpływu na prawa i wolności osób fizycznych i prawdopodobieństwo jego wystąpienia. Oczywiście ryzyko wzrasta, gdy konsekwencje naruszenia są poważniejsze, jak również wtedy, gdy wzrasta prawdopodobieństwo ich wystąpienia. W przypadku jakichkolwiek wątpliwości administrator powinien zgłosić naruszenie, nawet jeśli taka ostrożność mogłaby się okazać nadmierna. W załączniku B przedstawiono użyteczne przykłady różnych rodzajów naruszeń skutkujących ryzykiem lub wysokim ryzykiem dla osób fizycznych.

Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA) opracowała zalecenia dotyczące metod oceny wagi naruszenia, które mogą się przydać administratorom i podmiotom przetwarzającym podczas opracowywania planów działania i zarządzania w sytuacji wystąpienia naruszenia[42].

[42] ENISA, Zalecenia dotyczące metod oceny wagi naruszeń ochrony danych osobowych: https://www.enisa.europa.eu/publications/dbn-severity

V. Rozliczalność i prowadzenie dokumentacji

A. Dokumentowanie naruszeń

Bez względu na to, czy należy zgłosić dane naruszenie organowi nadzorczemu, czy też nie, administrator jest zobowiązany do dokumentowania wszystkich naruszeń, jak wyjaśniono w art. 33 ust. 5:

„Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu na weryfikowanie przestrzegania niniejszego artykułu".

Jest to powiązane z zasadą rozliczalności zawartą w art. 5 ust. 2. RODO. Wymóg dokumentowania zarówno naruszeń, których nie trzeba zgłaszać, jak i naruszeń, które zgłaszać trzeba, jest również związany z obowiązkami administratora określonymi w art. 24, a organ nadzorczy może zażądać wglądu do tej dokumentacji. Administratorzy powinni zatem stworzyć wewnętrzny rejestr naruszeń bez względu na to, czy muszą je zgłaszać, czy też nie[43].

Chociaż administrator określa metody i strukturę dokumentowania naruszeń, we wszystkich przypadkach należy uwzględnić określone kluczowe elementy zapisywanych informacji. Zgodnie z art. 33 ust. 5 administrator jest zobowiązany do rejestrowania szczegółowych informacji na temat naruszenia, które obejmują jego przyczyny, przebieg wydarzeń oraz zakres danych osobowych, których dotyczyło naruszenie. Powinny one obejmować również skutki i konsekwencje naruszenia, uwzględniając działania zaradcze podjęte przez administratora.

W przepisach RODO nie sprecyzowano okresu przechowywania takiej dokumentacji. W przypadku gdy takie zapisy zawierają dane osobowe, administrator musi określić właściwy okres przechowywania zgodnie z zasadami dotyczącymi przetwarzania danych osobowych[44] oraz podstawą prawną przetwarzania[45]. Musi on przechowywać dokumentację zgodnie z art. 33 ust. 5 w zakresie, w jakim może zostać wezwany do przedstawienia organowi nadzorczemu dowodów na przestrzeganie przepisów tego artykułu lub, w ujęciu bardziej ogólnym, zasady rozliczalności. W przypadku gdy dokumentacja nie zawiera żadnych danych osobowych, ustanowiona w RODO zasada ograniczenia przechowywania oczywiście nie ma zastosowania[46].

Grupa Robocza Art. 29 zaleca, aby poza tymi informacjami szczegółowymi administrator dokumentował również uzasadnienia decyzji podjętych w odpowiedzi na naruszenie. Uzasadnienie decyzji należy udokumentować w szczególności w przypadku niezgłoszenia naruszenia. Uzasadnienie powinno obejmować powody, dla których administrator uznał, że jest mało prawdopodobne, by naruszenie to mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych[47]. Jeżeli

[43] Administrator może podjąć decyzję o dokumentowaniu naruszeń w prowadzonym na podstawie art. 30 rejestrze czynności przetwarzania. Nie ma konieczności prowadzenia odrębnego rejestru pod warunkiem, że informacje dotyczące naruszenia są wyraźnie oznaczone i można je pobrać na żądanie.

[44] Zob. art. 5.

[45] Zobacz art. 6 oraz art. 9.

[46] Zob. art. 5 ust. 1 lit. e).

[47] Zob. motyw 85.

natomiast administrator uznał, że spełnione zostały którekolwiek warunki określone w art. 34 ust. 3, powinien być w stanie przedstawić wystarczające dowody potwierdzające.

W przypadku gdy administrator zgłasza naruszenie organowi nadzorczemu, lecz robi to z opóźnieniem, administrator musi przedstawić przyczyny takiego opóźnienia; stosowna dokumentacja może pomóc w wykazaniu, że opóźnienie w zgłoszeniu naruszenia jest uzasadnione i nie jest nadmierne.

Powiadamiając o naruszeniu osoby fizyczne, na które wywiera ono wpływ, administrator powinien zachować w tej kwestii przejrzystość i przekazać informacje w sposób sprawny i terminowy. Przechowywanie dowodów takiego powiadamiania ułatwi również administratorowi wykazanie swojej rozliczalności i zgodności z przepisami.

Zarówno administratorom, jak i podmiotom przetwarzającym łatwiej będzie przestrzegać przepisów art. 33 i 34, jeżeli wdrożą udokumentowaną procedurę powiadamiania, w której określone zostaną procesy postępowania po wykryciu naruszenia, jak również metody ograniczenia skutków incydentu, zarządzania nim i przywrócenia stanu sprzed jego wystąpienia, a także metody oceny ryzyka i zgłaszania naruszenia. W tym kontekście w wykazaniu zgodności z RODO pomocne może być również wykazanie, że pracownicy zostali poinformowani o istnieniu takich procedur i mechanizmów oraz że wiedzą, jak reagować na naruszenia.

Należy przy tym również podkreślić, że niewywiązanie się z obowiązku właściwego udokumentowania naruszenia może spowodować, że organ nadzorczy wykorzysta swoje uprawnienia na mocy art. 58 lub nałoży administracyjną karę pieniężną zgodnie z art. 83.

B. Rola inspektora ochrony danych

Administrator lub podmiot przetwarzający może wyznaczyć inspektora ochrony danych[48] – zgodnie z wymogami art. 37 albo dobrowolnie w ramach dobrej praktyki. W art. 39 RODO określono szereg zadań wchodzących w zakres obowiązków inspektora ochrony danych, co jednak nie uniemożliwia przydzielenia mu – w stosownych przypadkach – dodatkowych zadań przez podmiot przetwarzający.

Do zadań wchodzących w zakres obowiązków inspektora ochrony danych, które są szczególnie istotne z punktu widzenia zgłaszania naruszenia – obok innych obowiązków – należą: przekazywanie administratorowi lub podmiotowi przetwarzającemu zaleceń oraz informacji dotyczących ochrony danych, monitorowanie przestrzegania przepisów RODO oraz przekazywanie zaleceń w zakresie ocen skutków dla ochrony danych. Inspektor ochrony danych musi również współpracować z organem nadzorczym i służyć jako punkt kontaktowy dla organu nadzorczego i osób, których dane dotyczą. Należy również podkreślić, że zgodnie z art. 33 ust. 3 lit. b) podczas zgłaszania naruszenia organowi nadzorczemu administrator musi przekazać imię i nazwisko oraz dane kontaktowe swojego inspektora ochrony danych lub innego punktu kontaktowego.

W kwestii dokumentowania naruszeń administrator lub podmiot przetwarzający mogą rozważyć zasięgnięcie opinii swojego inspektora ochrony danych na temat struktury i przygotowania dokumentacji oraz zarządzania nią. Inspektor ochrony danych może również otrzymać dodatkowe zadanie polegające na prowadzeniu takich rejestrów.

Z powyższych czynników wynika, że inspektor ochrony danych powinien odgrywać kluczową rolę we wspieraniu zapobiegania naruszeniom lub przygotowaniu na wypadek ich wystąpienia poprzez wydawanie zaleceń i monitorowanie przestrzegania przepisów, jak również w sytuacji naruszenia (tj. podczas zgłaszania naruszenia organowi nadzorczemu) oraz podczas wszelkich dalszych postępowań

[48] Zob. wytyczne Grupy Roboczej dotyczące inspektorów ochrony danych dostępne pod adresem: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048

prowadzonych przez organ nadzorczy. W tym kontekście Grupa Robocza Art. 29 zaleca niezwłoczne informowanie inspektora ochrony danych o wystąpieniu naruszenia oraz angażowanie go na wszystkich etapach procesu zarządzania w sytuacji wystąpienia naruszenia oraz procesu zgłaszania naruszenia.

VI. Obowiązki zgłaszania określone w innych instrumentach prawnych

Poza zgłaszaniem naruszeń i powiadamianiem o nich na podstawie RODO i niezależnie od tych działań administratorzy powinni również posiadać wiedzę na temat wszelkich wymogów w zakresie zgłaszania incydentów bezpieczeństwa na podstawie innego powiązanego prawodawstwa, które może w ich przypadku mieć zastosowanie, a także wiedzę na temat tego, czy są na tej podstawie również zobowiązani do jednoczesnego zgłoszenia naruszenia ochrony danych osobowych organowi nadzorczemu. Poszczególne państwa członkowskie mogą nakładać takie wymogi w różnych postaciach, lecz jako przykładowe wymogi zgłaszania naruszeń zawarte w innych instrumentach prawnych oraz ich współzależności z RODO można wymienić:

- rozporządzenie (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (rozporządzenie eIDAS)[49]

W art 19 ust. 2 rozporządzenia eIDAS nałożono na dostawców usług zaufania wymóg zawiadamiania organu nadzoru o wszelkich przypadkach naruszenia bezpieczeństwa lub utraty integralności, które mają znaczący wpływ na świadczoną usługę zaufania lub przetwarzane w jej ramach dane osobowe. W stosownych przypadkach – tj. gdy tego rodzaju naruszenie lub utrata stanowią również naruszenie ochrony danych osobowych zgodnie z RODO – dostawca usług zaufania powinien również zgłosić naruszenie organowi nadzorczemu.

- dyrektywę (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (dyrektywa dotycząca cyberbezpieczeństwa)[50]

W art. 14 i 16 dyrektywy dotyczącej cyberbezpieczeństwa nałożono na operatorów usług kluczowych oraz na dostawców usług cyfrowych obowiązek zgłaszania incydentów bezpieczeństwa właściwemu organowi. Zgodnie z motywem 63 dyrektywy dotyczącej cyberbezpieczeństwa[51] incydenty bezpieczeństwa często wiążą się z niebezpieczeństwem naruszenia danych osobowych. Chociaż w dyrektywie dotyczącej cyberbezpieczeństwa nałożono na właściwe organy i organy nadzorcze wymóg współpracy i wymiany informacji w tym kontekście, pozostaje faktem, że w przypadku gdy takie incydenty stanowią naruszenie ochrony danych osobowych zgodnie z RODO lub w momencie gdy się nim stają, wspomniani operatorzy lub dostawcy musieliby zawiadomić organ nadzorczy niezależnie od wymogów dotyczących zgłoszenia incydentu zawartych w dyrektywie dotyczącej cyberbezpieczeństwa.

[49] Zob.: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32014R0910

[50] Zob.: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32016L1148

51 Motyw 63: *„ W wielu przypadkach istnieje niebezpieczeństwo naruszenia danych osobowych w wyniku incydentów. W tym kontekście właściwe organy oraz organy ochrony danych powinny ze sobą współpracować oraz wymieniać się informacjami dotyczącymi wszystkich istotnych kwestii w celu rozwiązywania problemów związanych z wszelkimi przypadkami naruszeń danych osobowych w wyniku incydentów”.*

Przykład

Dostawca usługi przetwarzania w chmurze, który zgłasza naruszenie na podstawie dyrektywy dotyczącej cyberbezpieczeństwa, może również mieć obowiązek powiadomienia administratora, jeżeli naruszenie to obejmuje naruszenie ochrony danych osobowych. Podobnie dostawca usług zaufania, który zgłasza naruszenie na podstawie rozporządzenia eIDAS, może być również zobowiązany do powiadomienia odpowiedniego organu ochrony danych, jeżeli doszło do naruszenia.

- dyrektywę 2009/136/WE (dyrektywa w sprawie praw obywateli) oraz rozporządzenie nr 611/2013 (rozporządzenie w sprawie powiadamiania o przypadkach naruszenia danych osobowych).

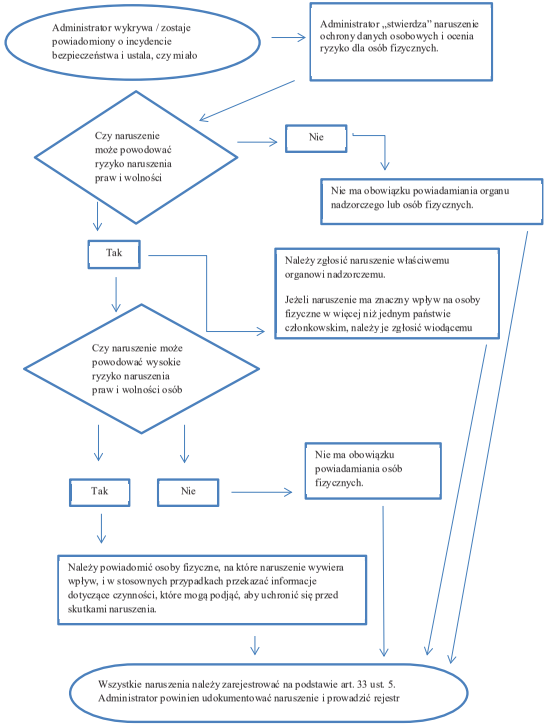
W kontekście dyrektywy 2002/58/WE[52] dostawcy publicznie dostępnych usług łączności elektronicznej są zobowiązani do zgłaszania naruszeń właściwym organom krajowym.

Administratorzy powinni mieć również świadomość wszelkich dodatkowych spoczywających na nich obowiązków zgłaszania naruszeń o charakterze prawnym, medycznym lub zawodowym przewidzianych w ramach pozostałych mających zastosowanie systemów.

[52] W dniu 10 stycznia 2017 r. Komisja Europejska przedstawiła wniosek dotyczący rozporządzenia w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej, które zastąpi dyrektywę 2009/136/WE i zlikwiduje wymogi zgłaszania naruszeń. Jednak do czasu przyjęcia tego wniosku przez Parlament Europejski wciąż obowiązywać będzie istniejący wymóg zgłaszania naruszeń, zob.: https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications

VII. Załącznik

A. Schemat ilustrujący wymogi zgłaszania naruszeń



B. Przykłady naruszeń ochrony danych osobowych i podmiotów, które należy poinformować

Poniższy niewyczerpujący wykaz przykładowych sytuacji pomoże administratorom określić, czy w poszczególnych scenariuszach naruszenia ochrony danych osobowych należy dokonać zgłoszenia. Przykłady te mogą również pomóc odróżnić „ryzyko" od „wysokiego ryzyka" naruszenia praw i wolności osób fizycznych.

Przykład	**Czy należy zgłosić naruszenie organowi nadzorczemu?**	**Czy należy zgłosić naruszenie osobie, której dane dotyczą?**	**Uwagi/zalecenia**
i. Administrator przechowywał zaszyfrowaną kopię bezpieczeństwa archiwum danych osobowych na pamięci USB. Pamięć ukradziono podczas włamania.	Nie.	Nie.	Jeżeli dane zostały zaszyfrowane za pomocą najnowocześniejszego algorytmu, utworzono kopie bezpieczeństwa danych, unikalny klucz nie został złamany, a dane można przywrócić w odpowiednim czasie – być może naruszenie to nie podlega zgłoszeniu. Jeżeli jednak w późniejszym czasie klucz zostanie złamany, sytuacja ta będzie wymagała zgłoszenia.
ii. Administrator prowadzi usługą internetową. W wyniku cyberataku na tę usługę nastąpił wyciek danych osobowych osób fizycznych. Klienci administratora znajdują się w jednym państwie członkowskim.	Tak, naruszenie należy zgłosić organowi nadzorczemu, jeżeli możliwe są konsekwencje dla osób fizycznych.	Tak, naruszenie należy zgłosić osobom fizycznym w zależności od charakteru danych osobowych, których dotyczy naruszenie, oraz gdy możliwe konsekwencje dla osób fizycznych są poważne.	
iii. Krótkotrwała, kilkuminutowa awaria systemu zasilania w centrum obsługi telefonicznej administratora, w wyniku której klienci nie mogą skontaktować się z administratorem i uzyskać dostępu do swoich danych.	Nie.	Nie.	Naruszenie to nie podlega zgłoszeniu, lecz mino to należy ten incydent zarejestrować na podstawie art. 33 ust. 5. Administrator musi prowadzić odpowiednie rejestry.
iv. Administrator pada ofiarą ataku za pomocą oprogramowania typu ransomware, w wyniku którego wszystkie dane zostały zaszyfrowane. Nie są dostępne żadne kopie bezpieczeństwa, a danych nie można przywrócić. W trakcie postępowania okazuje się, że oprogramowanie typu ransomware wykorzystano jedynie do zaszyfrowania danych, a w systemie nie stwierdzono obecności żadnego innego złośliwego oprogramowania.	Tak, naruszenie należy zgłosić organowi nadzorczemu, jeżeli możliwe są konsekwencje dla osób fizycznych, ponieważ sytuacja ta jest równoznaczna z utratą dostępności.	Tak, naruszenie należy zgłosić osobom fizycznym w zależności od charakteru danych osobowych, których dotyczy naruszenie, potencjalnych skutków braku dostępności danych oraz innych możliwych konsekwencji.	Jeżeli istniałaby kopia bezpieczeństwa i możliwe byłoby przywrócenie danych w odpowiednim czasie, zgłaszanie naruszenia organowi nadzorczemu lub osobom fizycznym nie byłoby konieczne, ponieważ nie miałyby miejsca trwała utrata dostępności lub naruszenie poufności danych. Jeżeli jednak organ nadzorczy dowiedziałby się o tym incydencie z innych źródeł, mógłby rozważyć wszczęcie postępowania do celów oceny zgodności z szerszymi wymogami dotyczącymi bezpieczeństwa określonymi w art. 32.
v. Pewna osoba dzwoni do centrum obsługi telefonicznej banku, by zgłosić naruszenie ochrony danych. Osoba ta otrzymała miesięczny wyciąg bankowy przeznaczony dla kogoś innego. Administrator przeprowadza krótkie postępowanie (tj. trwające do 24 godzin) i ustala z uzasadnioną pewnością, że miało miejsce naruszenie ochrony danych osobowych, i stwierdza, czy w jego systemie występuje wada, która może oznaczać, że naruszenie wpłynęło lub mogło wpłynąć na	Tak.	Naruszenie zgłasza się wyłącznie osobom fizycznym, na które naruszenie wywarło wpływ, jeżeli istnieje wysokie ryzyko i jest jasne, że naruszenie nie dotyczy nikogo innego.	Jeżeli w wyniku dalszego postępowania stwierdzono, że naruszenie ma wpływ na większą liczbę osób fizycznych, należy przekazać organowi nadzorczemu aktualne informacje, a administrator wykonuje dodatkową czynność polegającą na zawiadomieniu o naruszeniu innych osób fizycznych, jeżeli sytuacja ta może powodować dla nich wysokie ryzyko.

inne osoby fizyczne.			
vi. Administrator prowadzi internetową platformę handlową, a jego klienci znajdują się w wielu państwach członkowskich. Platforma pada ofiarą cyberataku i atakujący publikuje w internecie identyfikatory użytkownika, hasła i historię zakupów.	Tak, naruszenie należy zgłosić wiodącemu organowi nadzorczemu, jeżeli ma miejsce transgraniczne przetwarzanie.	Tak, ponieważ może to doprowadzić do powstania wysokiego ryzyka.	Administrator powinien zareagować, np. wymusić zmianę haseł kont, których dotyczy naruszenie, jak również poczynić inne kroki w celu zminimalizowania ryzyka. Administrator powinien również wziąć pod uwagę wszelkie inne wymogi zgłaszania naruszeń, np. wynikające z dyrektywy dotyczącej cyberbezpieczeństwa, które mają do niego zastosowanie z uwagi na fakt, że jest dostawcą usług cyfrowych.
vii. Przedsiębiorstwo zajmujące się web hostingiem, które pełni rolę podmiotu przetwarzającego, znajduje błąd w kodzie, który kontroluje autoryzację użytkowników. W wyniku tej wady każdy użytkownik może uzyskać wgląd w szczegółowe informacje na temat konta dowolnego innego użytkownika.	Jako podmiot przetwarzający przedsiębiorstwo zajmujące się web hostingiem musi niezwłocznie zgłosić naruszenie swoim klientom, na których wywarło ono wpływ (administratorom). Zakładając, że przedsiębiorstwo zajmujące się web hostingiem przeprowadziło swoje własne postępowanie, administratorzy, na których naruszenie wywarło wpływ, powinni mieć wystarczającą pewność co do tego, czy padli ofiarą naruszenia, a tym samym tego, czy można uznać, że „stwierdzili naruszenie" po	Jeżeli prawdopodobieństwo istnienia wysokiego ryzyka dla osób fizycznych jest niewielkie, nie ma potrzeby ich powiadomienia.	Przedsiębiorstwo zajmujące się web hostingiem (podmiot przetwarzający) musi również uwzględnić wszelkie inne obowiązki zgłaszania naruszeń (np. wynikające z dyrektywy dotyczącej cyberbezpieczeństwa – z uwagi na fakt, że jest dostawcą usług cyfrowych). Jeżeli nie nie wskazuje na to, że tę lukę w zabezpieczeniach wykorzystano przeciwko jakiemukolwiek administratorowi, naruszenie mogło nie podlegać zgłoszeniu, lecz prawdopodobnie należy je udokumentować lub jest związane z nieprzestrzeganiem art. 32.

	zgłoszeniu naruszenia przez przedsiębiorstwo zajmujące się web hostingiem (podmiot przetwarzający). Administrator musi następnie zgłosić naruszenie organowi nadzorczemu.		
viii. Szpitalna dokumentacja medyczna jest niedostępna przez 30 godzin w wyniku cyberataku.	Tak, szpital ma obowiązek zgłoszenia naruszenia, ponieważ może powstać wysokie ryzyko dla dobrostanu i prywatności pacjentów.	Tak, naruszenie należy zgłosić osobom fizycznym, na które wywiera ono wpływ.	
ix. Dane osobowe znacznej liczby studentów omyłkowo wysłano do niewłaściwej listy adresowej, na której znajduje się ponad 1000 odbiorców.	Tak, naruszenie należy zgłosić organowi nadzorczemu.	Tak, naruszenie należy zgłosić osobom fizycznym w zależności od zakresu i rodzaju ujawnionych danych osobowych i wagi możliwych konsekwencji.	
x. Wiadomość e-mail w ramach marketingu bezpośredniego wysłano do odbiorców w polach „do:" lub „dw:", tym samym umożliwiając każdemu odbiorcy wgląd w adresy e-mail innych odbiorców.	Tak, zgłoszenie naruszenia organowi nadzorczemu może być obowiązkowe, jeżeli naruszenie dotyczy dużej liczby osób, jeżeli ujawniono dane wrażliwe (takie jak np. lista adresowa psychoterapeuty) lub jeżeli inne czynniki stwarzają wysokie ryzyko (np. wiadomość e-mail zawiera hasła startowe).	Tak, naruszenie należy zgłosić osobom fizycznym w zależności od zakresu i rodzaju ujawnionych danych osobowych i wagi możliwych konsekwencji.	Zgłoszenie może nie być konieczne, jeżeli nie ujawniono żadnych danych wrażliwych i jeżeli ujawniono tylko niewielką liczbę adresów e-mail.

GRUPA ROBOCZA DS. OCHRONY DANYCH ART. 29



17/PL

WP 253

Wytyczne w sprawie stosowania i ustalania administracyjnych kar pieniężnych do celów rozporządzenia nr 2016/679

Przyjęte w dniu 3 października 2017 r.

Niniejsza grupa robocza została powołana na mocy art. 29 dyrektywy 95/46/WE. Jest to niezależny europejski organ doradczy w kwestiach ochrony danych i prywatności. Jego zadania zostały opisane w art. 30 dyrektywy 95/46/WE i art. 15 dyrektywy 2002/58/WE.

Obsługę sekretariatu zapewnia Dyrekcja C (Prawa Podstawowe i Obywatelstwo Unii Europejskiej)) Dyrekcji Generalnej ds. Sprawiedliwości Komisji Europejskiej, B-1049 Bruksela, Belgia, biuro nr MO-59 03/075.

Strona internetowa: http://ec.europa.eu/justice/data-protection/index_en.htm

GRUPA ROBOCZA DS. OCHRONY OSÓB FIZYCZNYCH W ZAKRESIE PRZETWARZANIA DANYCH OSOBOWYCH

powołana na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r.,

uwzględniając art. 29 i 30 tej dyrektywy,

uwzględniając swój regulamin wewnętrzny,

PRZYJMUJE NINIEJSZE WYTYCZNE:

Spis treści:

I. Wprowadzenie 4
II. Zasady 5
III. Kryteria oceny określone w art. 83 ust. 2 9
IV. Wniosek 18

I. Wprowadzenie

UE zakończyła kompleksową reformę rozporządzenia o ochronie danych w Europie. Reforma opiera się na kilku filarach (kluczowych elementach): spójnych zasadach, uproszczonych procedurach, skoordynowanych działaniach, zaangażowaniu użytkowników, skuteczniejszym informowaniu i silniejszych uprawnieniach wykonawczych.

Administratorzy danych i podmioty przetwarzające dane mają większe obowiązki w zakresie zapewnienia skutecznej ochrony danych osobowych osób fizycznych. Organy nadzorcze są uprawnione do zapewnienia przestrzegania zasad ogólnego rozporządzenia o ochronie danych (zwanego dalej „rozporządzeniem"), a także praw osób fizycznych, których dane osobowe są lub mogą być przetwarzane, zgodnie z jego literą i duchem.

Konsekwentne egzekwowanie zasad ochrony danych ma kluczowe znaczenie dla zharmonizowanego systemu ochrony danych. Administracyjne kary pieniężne są zasadniczym elementem nowego systemu egzekwowania wprowadzonego na mocy rozporządzenia, stanowiąc tym samym wraz z innymi środkami przewidzianymi w art. 58 istotną część zestawu narzędzi umożliwiających egzekwowanie prawa przez organy nadzorcze.

Niniejszy dokument jest przeznaczony do użytku organów nadzorczych w celu zapewnienia lepszego stosowania i egzekwowania rozporządzenia oraz wyraża wspólne rozumienie przepisów art. 83 rozporządzenia, a także ich współzależność z art. 58 i 70 oraz odpowiednimi motywami.

W szczególności, zgodnie z art. 70 ust. 1 lit. e), Europejska Rada Ochrony Danych jest uprawniona do wydawania wytycznych i zaleceń oraz określania najlepszych praktyk, by zachęcić do spójnego stosowania tego rozporządzenia, a art. 70 ust. 1 lit. k) stanowi podstawę do wydawania wytycznych dotyczących ustalania wysokości administracyjnych kar pieniężnych.

Wytyczne te nie są ani wyczerpujące, ani nie zawierają wyjaśnień co do różnic występujących między systemami prawa administracyjnego, cywilnego i karnego, jeżeli chodzi o nakładanie kar administracyjnych w ogólności.

W celu osiągnięcia spójnego podejścia do kwestii nakładania administracyjnych kar pieniężnych, które to podejście w odpowiedni sposób uwzględnia wszystkie zasady zawarte w niniejszych wytycznych, Europejska Rada Ochrony Danych uzgodniła wspólne rozumienie kryteriów oceny ujętych w art. 83 ust. 2 rozporządzenia. Europejska Rada Ochrony Danych i poszczególne organy nadzorcze zobowiązują się do stosowania niniejszych wytycznych jako wspólnego podejścia.

II. Zasady

W przypadku gdy w oparciu o ocenę okoliczności faktycznych sprawy zostanie stwierdzone naruszenie rozporządzenia, właściwy organ nadzorczy obowiązany jest wskazać najodpowiedniejszy środek naprawczy (najodpowiedniejsze środki naprawcze) w celu zaradzenia takiemu naruszeniu. Przepisy art. 58 ust. 2 lit. b)–j)[1] określają działania, które organy nadzorcze mogą podejmować w przypadku nieprzestrzegania odpowiednich przepisów przez administratora lub podmiot przetwarzający. Korzystając ze wskazanych uprawnień, organy nadzorcze mają obowiązek przestrzegać następujących zasad:

1. Naruszenie rozporządzenia powinno prowadzić do nałożenia „równoważnych kar".

Pojęcie „równoważności" ma zasadnicze znaczenie dla określenia zakresu obowiązków organów nadzorczych w celu zapewnienia spójności w korzystaniu z uprawnień naprawczych zgodnie z art. 58 ust. 2 w ogóle, a w szczególności w odniesieniu do stosowania administracyjnych kar pieniężnych[2].

Aby zapewnić wysoki i spójny stopień ochrony osób fizycznych oraz usunąć przeszkody w przepływie danych osobowych w Unii, ***należy zapewnić równorzędny stopień ochrony*** *we wszystkich państwach członkowskich* (motyw 10). Motyw 11 wyjaśnia, że równorzędny stopień ochrony danych osobowych w Unii wymaga m.in. „*równorzędnych uprawnień w zakresie monitorowania i egzekwowania przepisów o ochronie danych osobowych oraz równorzędnych kar za naruszenia tych przepisów w państwach członkowskich*". Ponadto równorzędne kary w państwach członkowskich oraz skuteczna współpraca organów nadzorczych różnych państw członkowskich są postrzegane jako środki „*zapobiegania rozbieżnościom hamującym swobodny przepływ danych osobowych na rynku wewnętrznym*", zgodnie z motywem 13 rozporządzenia.

Rozporządzenie ustanawia solidniejszą podstawę zapewnienia większej spójności niż dyrektywa 95/46/WE, gdyż jest ono bezpośrednio stosowane w państwach członkowskich. Podczas gdy organy nadzorcze działają „w sposób w pełni niezależny" (art. 52) w odniesieniu do rządów krajowych, administratorów lub podmiotów przetwarzających, mają one obowiązek współpracować „*w celu zapewnienia spójnego stosowania i egzekwowania niniejszego rozporządzenia*" (art. 57 ust. 1 lit. g)).

W rozporządzeniu wymaga się większej spójności w zakresie nakładania kar niż w dyrektywie 95/46. W sprawach transgranicznych spójność osiąga się przede wszystkim poprzez zastosowanie mechanizmu kompleksowej współpracy oraz w pewnym stopniu mechanizmu spójności określonego w nowym rozporządzeniu.

W przypadkach krajowych objętych rozporządzeniem organy nadzorcze będą stosować niniejsze wytyczne w duchu współpracy zgodnie z art. 57 ust. 1 lit. g) i art. 63 w celu zapewnienia spójnego stosowania i egzekwowania rozporządzenia. Chociaż organy nadzorcze zachowują niezależność w, wyborze środków naprawczych wymienionych w art. 58 ust. 2, należy unikać sytuacji, w których organy nadzorcze w podobnych sprawach stosują różne środki naprawcze.

[1] Artykuł 58 ust. 2 lit. a) stanowi, że ostrzeżenia mogą być wydawane w odniesieniu do „możliwości naruszenia przepisów niniejszego rozporządzenia poprzez planowane operacje przetwarzania". Innymi słowy, w sprawie objętej przepisem nie doszło jeszcze do naruszenia rozporządzenia.

[2] Nawet jeżeli systemy prawne w niektórych krajach UE nie przewidują nakładania administracyjnych kar pieniężnych określonych w rozporządzeniu, takie stosowanie zasad we wspomnianych państwach członkowskich musi mieć skutek równoważny administracyjnym karom pieniężnym nakładanym przez organy nadzorcze (motyw 151). Sądy są związane rozporządzeniem, lecz nie są związane wytycznymi Europejskiej Rady Ochrony Danych.

Ta sama zasada obowiązuje, gdy owymi środkami naprawczymi są nakładane kary.

2. Podobnie jak wszystkie środki naprawcze wybierane przez organy nadzorcze, administracyjne kary pieniężne winny być „skuteczne, proporcjonalne i odstraszające".

Podobnie jak wszelkie środki naprawcze w ogólności, administracyjne kary pieniężne powinny w stosowny sposób odpowiadać charakterowi, wadze i konsekwencjom naruszenia, a organy nadzorcze muszą dokonywać oceny okoliczności faktycznych danej sprawy w sposób spójny i obiektywnie uzasadniony. Ocena tego, co jest skuteczne, proporcjonalne i odstraszające, w każdym przypadku będzie musiała również odzwierciedlać cel wybranego środka naprawczego, którym jest przywrócenie zgodności z przepisami lub ukaranie za bezprawne zachowanie (lub oba te cele).

Organy nadzorcze powinny określić środek naprawczy, który jest „*skuteczny, proporcjonalny i odstraszający*" (art. 83 ust. 1) zarówno w sprawach krajowych (art. 55), jak i w sprawach związanych z transgranicznym przetwarzaniem danych osobowych (jak określono w art. 4 ust. 23).

W niniejszych wytycznych uznano, że prawodawstwo krajowe może wprowadzić dodatkowe wymogi w zakresie prowadzenia przez organy nadzorcze postępowania przymuszającego. Mogą one przykładowo obejmować powiadomienia adresowe, formę, terminy składania oświadczeń, środki odwoławcze, egzekucję, uiszczanie płatności[3].

Takie wymogi nie powinny jednak w praktyce utrudniać osiągnięcia skuteczności, proporcjonalności lub odstraszającego charakteru stosowanych środków naprawczych.

Bardziej precyzyjne określenie skuteczności, proporcjonalności lub odstraszającego charakteru przyniesie rozwijająca się praktyka samych organów nadzorczych (w zakresie ochrony danych oraz doświadczenia organów w innych sektorach regulacyjnych), a także orzecznictwo zawierające wykładnię tych zasad.

W celu nałożenia skutecznych, proporcjonalnych i odstraszających kar pieniężnych organ nadzorczy stosuje definicję pojęcia przedsiębiorstwa przyjętą przez TSUE do celów stosowania art. 101 i 102 TFUE, a mianowicie, że poprzez pojęcie przedsiębiorstwa **należy rozumieć** jednostkę gospodarczą, którą może utworzyć spółka dominująca i wszystkie zaangażowane podmioty zależne. Zgodnie z prawem i orzecznictwem[4] UE przedsiębiorstwo jest tu rozumiane jako jednostka gospodarcza, która prowadzi działalność handlową/gospodarczą, bez względu na osobę prawną (motyw 150).

3. Właściwy organ nadzorczy dokonuje oceny „w każdym indywidualnym przypadku".

[3] Przykładowo ramy konstytucyjne i projektowane regulacje prawne w zakresie ochrony danych w Irlandii stanowią, że w sprawie samego naruszenia podjęta zostaje formalna decyzja, a o decyzji tej informuje się odpowiednie strony przed dokonaniem oceny skali kary (kar). Decyzji w sprawie samego naruszenia nie można zmienić podczas oceny skali kary (kar).

[4] Definicja sformułowana w orzecznictwie TSUE brzmi następująco: „pojęcie przedsiębiorstwa obejmuje każdy podmiot prowadzący działalność gospodarczą niezależnie od statusu prawnego podmiotu i sposobu, w jaki jest on finansowany" (sprawa Höfner i Elsner, pkt 21, ECLI:UE:C:1991:161). Pojęcie przedsiębiorstwa „winno być rozumiane jako odnoszące się do jednostki gospodarczej, nawet jeśli z prawnego punktu widzenia owa jednostka gospodarcza składa się z wielu osób fizycznych lub prawnych" (sprawa Confederación Española de Empresarios de Estaciones de Servicio, pkt 40, ECLI:EU:C:2006:784).

Administracyjne kary pieniężne mogą być nakładane w odpowiedzi na cały szereg naruszeń. Artykuł 83 rozporządzenia przewiduje zharmonizowane podejście do przypadków naruszenia obowiązków enumeratywnie wyliczonych w ust. 4–6. Prawo państw członkowskich może rozszerzyć stosowanie art. 83 na organy i podmioty publiczne ustanowione w konkretnym państwie członkowskim. Ponadto prawo państwa członkowskiego może dopuszczać — a nawet wydać upoważnienie — w zakresie nałożenia kary pieniężnej za naruszenie innych przepisów prawa niż art. 83 ust. 4–6.

Rozporządzenie wymaga dokonania oceny każdego przypadku z osobna[5]. Artykuł 83 ust. 2 stanowi punkt wyjścia dla przeprowadzenia takiej indywidualnej oceny. Ustęp ten stanowi, że *„decydując, czy nałożyć administracyjną karę pieniężną, oraz ustalając jej wysokość, zwraca się w każdym indywidualnym przypadku należytą uwagę na…"*. Stosownie do powyższego oraz w świetle motywu 148[6] organ nadzorczy jest odpowiedzialny za wybór najodpowiedniejszego środka (najodpowiedniejszych środków). W przypadkach, o których mowa w art. 83 ust. 4–6, wybór ten **musi** uwzględniać wszystkie środki naprawcze, w tym nałożenie odpowiedniej administracyjnej kary pieniężnej, czy to towarzyszącej środkowi naprawczemu na mocy art. 58 ust. 2, czy też występującej samodzielnie.

Kary pieniężne są ważnym narzędziem, które organy nadzorcze powinny stosować w odpowiednich okolicznościach. Zachęca się organy nadzorcze do stosowania rozważnego i wyważonego podejścia w zakresie stosowania środków naprawczych, tak aby reakcja na dane naruszenie była zarówno skuteczna i odstraszająca, jak również proporcjonalna. Celem nie jest tu traktowanie kar pieniężnych jako ostateczności, czy też powstrzymywanie się od ich stosowania, lecz nakładanie ich w sposób uniemożliwiający podważanie ich skuteczności jako narzędzia.

Europejska Rada Ochrony Danych, w sytuacjach gdy jest do tego upoważniona na mocy art. 65 rozporządzenia, wyda wiążącą decyzję w sprawie sporów między organami w kwestiach dotyczących przede wszystkim stwierdzenia istnienia naruszenia. W przypadku gdy istotny i uzasadniony sprzeciw wiąże się z kwestią zgodności środka naprawczego z wytycznymi ogólnego rozporządzenia o ochronie danych, w decyzji Europejskiej Rady Ochrony Danych określi się również sposób, w jaki

[5] W związku ze stosowaniem kryteriów określonych w art. 83 istnieją inne przepisy, które wzmacniają fundamenty takiego podejścia, a mianowicie:

- Motyw 141: *„Postępowanie wyjaśniające na podstawie skargi powinno być prowadzone – z zastrzeżeniem kontroli sądowej – w zakresie odpowiadającym konkretnej sprawie"*.
- Motyw 129: *„Swoje uprawnienia organy nadzorcze powinny wykonywać zgodnie z odpowiednimi zabezpieczeniami proceduralnymi przewidzianymi w prawie Unii i prawie państwa członkowskiego, bezstronnie, sprawiedliwie i w rozsądnym terminie. W szczególności każdy środek powinien być odpowiedni, niezbędny i proporcjonalny, aby zapewnić przestrzeganie niniejszego rozporządzenia – z uwzględnieniem okoliczności danej sprawy… "*.
- Artykuł 57 ust. 1 lit f): *„rozpatruje skargi wniesione przez osobę, której dane dotyczą, lub przez podmiot, organizację lub zrzeszenie zgodnie z art. 80, w odpowiednim zakresie prowadzi postępowania w przedmiocie tych spraw"*.

[6] *„Aby egzekwowanie przepisów niniejszego rozporządzenia było skuteczniejsze, należy za jego naruszenie nakładać sankcje, w tym administracyjne kary pieniężne – oprócz lub zamiast odpowiednich środków nakładanych na mocy niniejszego rozporządzenia przez organ nadzorczy. Jeżeli naruszenie jest niewielkie lub jeżeli grożąca kara pieniężna stanowiłaby dla osoby fizycznej nieproporcjonalne obciążenie, można zamiast tego udzielić upomnienia. Powinno się jednak zwrócić należytą uwagę na charakter, wagę oraz czas trwania naruszenia, na to, czy naruszenie nie było umyślne, na działania podjęte dla zminimalizowania szkody, na stopień odpowiedzialności lub wszelkie mające znaczenie wcześniejsze naruszenia, na sposób, w jaki organ nadzorczy dowiedział się o naruszeniu, na przestrzeganie środków nałożonych na administratora lub podmiot przetwarzający, na stosowanie kodeksów postępowania oraz wszelkie inne czynniki obciążające lub łagodzące. Nakładanie sankcji, w tym administracyjnych kar pieniężnych, powinno podlegać odpowiednim zabezpieczeniom proceduralnym zgodnym z ogólnymi zasadami prawa Unii i z Kartą praw podstawowych, w tym skutecznej ochronie prawnej i prawu do rzetelnego procesu"*.

zaproponowana przez właściwy organ nadzorczy w projekcie decyzji administracyjna kara pieniężna spełnia zasady skuteczności, proporcjonalności i odstraszania. Wytyczne Europejskiej Rady Ochrony Danych dotyczące stosowania art. 65 rozporządzenia w kontekście decyzji, którą ma podjąć Europejska Rada Ochrony Danych, będą przedmiotem osobnego szczegółowego omówienia.

4. Zharmonizowane podejście do administracyjnych kar pieniężnych w zakresie ochrony danych wymaga aktywnego udziału i wymiany informacji między organami nadzorczymi.

W niniejszych wytycznych uznaje się, że uprawnienia w zakresie nakładania kar pieniężnych są dla niektórych krajów nowością w dziedzinie ochrony danych, co z kolei wiąże się z wieloma kwestiami związanymi z zasobami, organizacją i ukształtowaniem postępowania. W szczególności od decyzji dotyczących wykonywania przez organy nadzorcze przyznanych im uprawnień w zakresie nakładania kar pieniężnych będzie można się odwołać do sądów krajowych.

Organy nadzorcze współpracują ze sobą oraz — w stosownych przypadkach — z Komisją Europejską przy wykorzystaniu mechanizmów współpracy określonych w rozporządzeniu w celu usprawnienia formalnej i nieformalnej wymiany informacji np. poprzez regularne warsztaty. Współpraca ta powinna opierać się na wymianie doświadczeń i praktyk w zakresie nakładania kar pieniężnych, tak aby ostatecznie wypracować większą spójność.

Ta proaktywna wymiana informacji, oprócz rozwijającego się orzecznictwa dotyczącego korzystania z takich uprawnień, może prowadzić do rewizji zasad lub poszczególnych szczegółów niniejszych wytycznych.

III. Kryteria oceny określone w art. 83 ust. 2

Artykuł 83 ust. 2 zawiera wykaz kryteriów, którymi organy nadzorcze powinny się posługiwać, przeprowadzając ocenę zarówno tego, czy należy nałożyć karę pieniężną, jak i określając jej wysokość. Regulacja ta nie zaleca dokonywania ponownej oceny tych samych kryteriów, lecz przeprowadzenie oceny uwzględniającej wszystkie okoliczności każdego indywidualnego przypadku zgodnie z art. 83[7].

Wnioski wyciągnięte na pierwszym etapie oceny mogą zostać wykorzystane w drugiej części dotyczącej wysokości kary, tym samym pozwalając uniknąć powtórnej oceny przy użyciu tych samych kryteriów.

Niniejsza sekcja zawiera wskazówki dla organów nadzorczych dotyczące sposobu interpretacji poszczególnych okoliczności faktycznych sprawy w świetle kryteriów określonych w art. 83 ust. 2.

a) Charakter, waga i czas trwania naruszenia

Zgodnie z rozporządzeniem prawie wszystkie obowiązki administratorów i podmiotów przetwarzających są podzielone na kategorie zgodnie z ich **charakterem** określonym w przepisach art. 83 ust. 4–6. Poprzez ustanowienie dwóch różnych maksymalnych wysokości administracyjnej kary pieniężnej (10/20 mln EUR) w rozporządzeniu wskazuje się, że naruszenie niektórych przepisów rozporządzenia może być poważniejsze niż naruszenie innych przepisów. Niemniej oceniając okoliczności faktyczne sprawy w świetle ogólnych kryteriów określonych w art. 83 ust. 2, właściwy organ nadzorczy może zdecydować, że w danym przypadku istnieje większa lub mniejsza potrzeba reagowania za pomocą środka naprawczego w formie kary pieniężnej. W przypadku gdy wybrano karę pieniężną jako jeden z wielu właściwych środków naprawczych, należy zastosować system klasyfikacji rozporządzenia (art. 83 ust. 4–6) w celu wskazania maksymalnej kary pieniężnej, którą można nałożyć zgodnie z charakterem omawianego naruszenia.

W motywie 148 wprowadza się pojęcie „niewielkich naruszeń". Takie naruszenia mogą odnosić się do pogwałcenia jednego lub kilku przepisów rozporządzenia wymienionych w art. 83 ust. 4 lub 5. Ocena kryteriów określonych w art. 83 ust. 2 może jednak skłonić organ nadzorczy do uznania, że w konkretnych okolicznościach danego przypadku dane naruszenie na przykład nie stanowi poważnego zagrożenia dla praw osób, których dane dotyczą, oraz nie wpływa na istotę danego obowiązku. W takich przypadkach karę pieniężną można (choć nie zawsze) zastąpić upomnieniem.

W motywie 148 nie przewiduje się obowiązku zastępowania przez organ nadzorczy kary pieniężnej każdorazowo upomnieniem w przypadku niewielkiego naruszenia (*„można zamiast tego udzielić upomnienia"*), a raczej wskazuje się na możliwość, z której można skorzystać po dokonaniu konkretnej oceny wszystkich okoliczności sprawy.

Motyw 148 stwarza taką samą możliwość zastąpienia kary pieniężnej upomnieniem w przypadku gdy administratorem danych jest osoba fizyczna, a grożąca kara pieniężna stanowiłaby dla osoby fizycznej nieproporcjonalne obciążenie. Punktem wyjścia jest tu ocena organu nadzorczego, czy — w świetle istniejących okoliczności sprawy — nałożenie kary jest konieczne. Jeżeli organ tak uzna, obowiązany jest również ocenić, czy grożąca kara pieniężna stanowiłaby dla osoby fizycznej nieproporcjonalne obciążenie.

W rozporządzeniu poszczególnym naruszeniom nie są przypisane konkretne kwoty, a jedynie określone są pułapy (kwoty maksymalne). Może to wskazywać na względnie niższą wagę naruszenia zobowiązań wymienionych w art. 83 ust. 4 w porównaniu z zobowiązaniami określonymi w art. 83 ust. 5. Skuteczna, proporcjonalna i odstraszająca reakcja na naruszenie art. 83 ust. 5 będzie jednak zależeć od okoliczności danej sprawy.

Niemniej należy zauważyć, że naruszenia przepisów rozporządzenia, które ze swej natury należą do kategorii „w wysokości do 10 mln EUR lub w wysokości do 2% jego całkowitego rocznego światowego obrotu", jak określono w art. 83 ust. 4, mogą w pewnych okolicznościach kwalifikować się do wyższej kategorii (20 mln EUR). Taka sytuacja może mieć miejsce, kiedy owe naruszenia były już wcześniej przedmiotem nakazu[8] orzeczonego przez organ nadzorczy, do którego to nakazu administrator lub podmiot przetwarzający się nie zastosowali[9] (art. 83 ust. 6). Przepisy prawa krajowego mogą w praktyce mieć wpływ na tę ocenę[10]. Charakter naruszenia, jak również *„zakres, cel danego przetwarzania, liczba poszkodowanych osób, których dane dotyczą, oraz rozmiar poniesionej przez nie szkody"* będą wskazywać na **wagę** naruszenia. Występowanie kilku różnych naruszeń popełnionych łącznie w konkretnym pojedynczym przypadku oznacza, że organ nadzorczy może nakładać administracyjne kary pieniężne w sposób, który jest zarazem skuteczny, proporcjonalny i odstraszający na poziomie najpoważniejszego naruszenia. Dlatego też w przypadku wykrycia naruszenia art. 8 i art. 12 organ nadzorczy może zastosować środki naprawcze określone w art. 83 ust. 5, które odpowiadają kategorii najpoważniejszego naruszenia, a mianowicie art. 12. Przedstawienie dalszych szczegółów na tym etapie wykracza poza zakres niniejszych wytycznych (szczegółowe wyliczenia mogłyby być przedmiotem kolejnego etapu opracowywania wytycznych).

Poniższe czynniki należy oceniać łącznie, np. liczbę osób, których dane dotyczą, wraz z potencjalnym wpływem na te osoby.

Należy ocenić **liczbę** osób, których dane dotyczą, w celu ustalenia, czy jest to pojedyncze zdarzenie, czy też mamy do czynienia z bardziej systematycznym naruszeniem lub brakiem odpowiednich sposobów postępowania. Nie oznacza to, że pojedyncze zdarzenie nie powinno być egzekwowane, gdyż nawet pojedyncze zdarzenie może mieć wpływ na dużą liczbę osób, których dane dotyczą. W zależności od okoliczności sprawy będzie to dotyczyć, odpowiednio, np. całkowitej liczby osób

[7] Ocena kary, jaka zostanie nałożona, może nadejść oddzielnie po dokonaniu oceny, czy doszło do naruszenia z powodu krajowych przepisów proceduralnych wynikających z wymogów konstytucyjnych w niektórych krajach. To z kolei może ograniczyć treść i ilość szczegółów w projekcie decyzji wydanym przez główny organ nadzorczy w takich krajach.

[8] Nakazy wymienione w art. 58 ust. 2 to:

- nakazanie administratorowi lub podmiotowi przetwarzającemu spełnienia żądania osoby, której dane dotyczą, wynikającego z praw przysługujących jej na mocy niniejszego rozporządzenia;
- nakazanie administratorowi lub podmiotowi przetwarzającemu dostosowania operacji przetwarzania do przepisów niniejszego rozporządzenia, a w stosownych przypadkach wskazanie sposobu i terminu;
- nakazanie administratorowi zawiadomienia osoby, której dane dotyczą, o naruszeniu ochrony danych;
- wprowadzanie czasowego lub całkowitego ograniczenia przetwarzania, w tym zakazu przetwarzania;
- nakazanie na mocy art. 16, 17 i 18 sprostowania lub usunięcia danych osobowych lub ograniczenia ich przetwarzania oraz nakazanie na mocy art. 17 ust. 2 i art. 19 powiadomienia o tych czynnościach odbiorców, którym dane osobowe ujawniono;
- nakazanie podmiotowi certyfikującemu cofnięcia certyfikacji udzielonej na mocy art. 42 lub 43, lub nakazanie podmiotowi certyfikującemu nieudzielania certyfikacji, jeżeli jej wymogi nie są spełnione lub przestały być spełniane;
- nakazanie zawieszenia przepływu danych do odbiorcy w państwie trzecim lub do organizacji międzynarodowej.

[9] Stosowanie art. 83 ust. 6 w sposób bezwzględny wymaga uwzględnienia krajowych przepisów postępowania. Prawo krajowe określa, w jaki sposób wydawany jest nakaz, jak jest on doręczany, od którego momentu zaczyna obowiązywać, czy istnieje okres karencji na jego przestrzeganie. W szczególności należy uwzględnić wpływ wniesienia środka odwoławczego na wykonalność nakazu.

[10] Przepisy ustawowe dotyczące przedawnienia mogą skutkować tym, że poprzedni nakaz organu nadzorczego może nie zostać uwzględniony z uwagi na czas, jaki upłynął od orzeczenia poprzedniego nakazu. W niektórych systemach prawnych przepisy wymagają, aby po upływie terminu przedawnienia nakazu nie można było nałożyć kary pieniężnej za nieprzestrzeganie tego nakazu zgodnie z art. 83 ust. 6. Od organu nadzorczego w systemie prawnym danego kraju zależeć będzie, w jaki sposób regulacje takie będą miały na niego wpływ.

rejestrujących się w danej bazie danych, liczby użytkowników usługi, liczby klientów lub populacji danego kraju.

Należy również ocenić **cel** przetwarzania. W opinii Grupy Roboczej Art. 29 w sprawie „ograniczenia celu"[11] przeanalizowano wcześniej dwa podstawowe elementy tej zasady w przepisach o ochronie danych: określenie celu i zgodne zastosowanie. Oceniając cel przetwarzania w kontekście art. 83 ust. 2, organy nadzorcze powinny określić, w jakim stopniu przetwarzanie spełnia dwa kluczowe elementy tej zasady[12]. W niektórych sytuacjach organ nadzorczy może uznać za konieczne, aby w analizie art. 83 ust. 2 uwzględnić głębszą analizę celu samego przetwarzania.

W przypadku gdy osoba, której dane dotyczą, poniosła **szkodę**, należy uwzględnić rozmiar poniesionej szkody. Przetwarzanie danych osobowych może generować ryzyko naruszenia praw i wolności danej osoby, co ilustruje motyw 75:

> *„Ryzyko naruszenia praw lub wolności osób, o różnym prawdopodobieństwie i wadze zagrożeń, może wynikać z przetwarzania danych osobowych mogącego prowadzić do uszczerbku fizycznego lub szkód majątkowych lub niemajątkowych, w szczególności: jeżeli przetwarzanie może poskutkować dyskryminacją, kradzieżą tożsamości lub oszustwem dotyczącym tożsamości, stratą finansową, naruszeniem dobrego imienia, naruszeniem poufności danych osobowych chronionych tajemnicą zawodową, nieuprawnionym odwróceniem pseudonimizacji lub wszelką inną znaczną szkodą gospodarczą lub społeczną; jeżeli osoby, których dane dotyczą, mogą zostać pozbawione przysługujących im praw i wolności lub możliwości sprawowania kontroli nad swoimi danymi osobowymi; jeżeli przetwarzane są dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, wyznanie lub przekonania światopoglądowe, lub przynależność do związków zawodowych oraz jeżeli przetwarzane są dane genetyczne, dane dotyczące zdrowia lub dane dotyczące seksualności lub wyroków skazujących i naruszeń prawa lub związanych z tym środków bezpieczeństwa; jeżeli oceniane są czynniki osobowe, w szczególności analizowane lub prognozowane aspekty dotyczące efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się— w celu tworzenia lub wykorzystywania profili osobistych; jeżeli przetwarzane są dane osobowe osób wymagających szczególnej opieki, w szczególności dzieci; lub jeżeli przetwarzanie dotyczy dużej ilości danych osobowych i wpływa na dużą liczbę osób, których dane dotyczą".*

Jeżeli szkoda została lub może zostać poniesiona z powodu naruszenia rozporządzenia, organ nadzorczy winien to uwzględnić przy wyborze środka naprawczego, chociaż sam organ nadzorczy nie jest właściwy do przyznania szczególnego odszkodowania za poniesioną szkodę.

Nałożenie kary pieniężnej nie zależy od zdolności organu nadzorczego do ustalenia związku przyczynowo-skutkowego pomiędzy naruszeniem a stratą materialną (zob. np. art. 83 ust. 6).

Czas trwania naruszenia może przykładowo świadczyć o:

a) celowym działaniu administratora danych;

b) braku podjęcia odpowiednich środków zapobiegawczych;

c) niemożności wprowadzenia wymaganych środków technicznych i organizacyjnych.

[11] Opinia nr 03/2013 WP 203 w sprawie ograniczenia celu dostępna jest na stronie internetowej: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

[12] Zob. także dokument grupy roboczej WP 217 dot. opinii nr 6/2014 w sprawie pojęcia prawnie uzasadnionych interesów administratora danych na mocy art. 7, a dokładnie odpowiedź na pytanie na str. 24: „Co sprawia, że interes jest »uzasadniony« lub »nieuzasadniony«?"

b) Umyślny lub nieumyślny charakter naruszenia

Zasadniczo „umyślność" obejmuje zarówno wiedzę, jak i celowe działanie, w związku z cechami charakterystycznymi czynu zabronionego, podczas gdy „nieumyślność" oznacza brak zamiaru spowodowania naruszenia, pomimo niedopełnienia przez administratora/podmiot przetwarzający obowiązku staranności wymaganego prawem.

Ogólnie uznaje się, że wykazujące pogardę wobec przepisów prawa umyślne naruszenia są poważniejsze niż te nieumyślne, a w konsekwencji częściej wiążą się z nałożeniem administracyjnej kary pieniężnej. Odpowiednie wnioski dotyczące umyślnego lub nieumyślnego charakteru naruszenia zostaną wyciągnięte na podstawie identyfikacji obiektywnych elementów działania zebranych w oparciu o okoliczności faktyczne sprawy. Ponadto rozwijające się orzecznictwo i praktyka w zakresie ochrony danych, do których zastosowanie ma rozporządzenie, wyeksponują okoliczności, które pozwolą wyodrębnić bardziej czytelne progi służące ocenie, czy dane naruszenie miało charakter umyślny.

Okolicznościami wskazującymi na umyślne naruszenia mogą być niezgodne z prawem przetwarzanie wyraźnie zatwierdzone przez ścisłe kierownictwo administratora lub – wbrew opinii inspektora ochrony danych lub wbrew istniejącym zasadom – na przykład uzyskiwanie i przetwarzanie danych o pracownikach u konkurenta z zamiarem zdyskredytowania tego konkurenta na rynku.

Innymi przykładami mogą być:

- zmiana danych osobowych w celu wywołania mylącego (pozytywnego) wrażenia dotyczącego rzekomego osiągnięcia celów — tak stało się w przypadku celów dotyczących okresów oczekiwania w szpitalach;
- handel danymi osobowymi w celach marketingowych, tj. sprzedaż danych jako „wybranych" bez sprawdzenia poglądów / ignorując poglądy osób, których dane dotyczą, w odniesieniu do sposobu użycia tych danych.

Innymi okolicznościami wskazującymi na zaniedbanie mogą być nieprzeczytanie i nieprzestrzeganie istniejących zasad, błąd ludzki, niesprawdzenie danych osobowych w opublikowanych źródłach, niedokonanie aktualizacji technicznych w odpowiednim czasie, nieprzyjęcie zasad (w przeciwieństwie do ich niestosowania).

Przedsiębiorstwa powinny być odpowiedzialne za przyjmowanie struktur i zasobów adekwatnych do charakteru i złożoności swej działalności. W związku z tym administratorzy i podmioty przetwarzające nie mogą uzasadniać naruszania przepisów o ochronie danych powołując się na niedobór zasobów. Podstawą procedur i dokumentacji działań związanych z przetwarzaniem jest podejście oparte na analizie ryzyka zgodnie z rozporządzeniem.

Istnieją szare obszary, które wpłyną na decyzję co do zastosowania/niezastosowania środka naprawczego. Wówczas organ być może uznać za niezbędne przeprowadzenie obszerniejszego dochodzenia w celu ustalenia okoliczności faktycznych sprawy i zapewnienia, że wszystkie szczególne okoliczności w każdym indywidualnym przypadku zostały należycie uwzględnione.

c) Działania podjęte przez administratora lub podmiot przetwarzający w celu zminimalizowania szkody poniesionej przez osoby, których dane dotyczą

Administratorzy danych i podmioty przetwarzające dane mają obowiązek wdrażania środków technicznych i organizacyjnych w celu zapewnienia poziomu bezpieczeństwa odpowiedniego do stopnia ryzyka, dokonywania oceny skutków dla ochrony danych oraz minimalizowania ryzyka naruszenia praw i wolności osób fizycznych wynikającego z przetwarzania danych osobowych. Jeżeli jednak dojdzie do naruszenia i osoba, której dane dotyczą, poniesie szkodę, strona odpowiedzialna powinna podjąć wszelkie możliwe starania celem ograniczenia skutków naruszenia dla danej osoby

(danych osób). Organ nadzorczy uwzględni taką odpowiedzialną postawę (lub brak takiej postawy) podczas dokonywania wyboru środka naprawczego (środków naprawczych) oraz przy ustalaniu wysokości kary pieniężnej mającej zastosowanie w konkretnym przypadku.

Pomimo szczególnej roli, jaką odgrywają czynniki obciążające i łagodzące w dostosowaniu wysokości kary pieniężnej do konkretnych okoliczności sprawy, nie należy umniejszać roli tych czynników w wyborze właściwego środka naprawczego. W przypadkach, w których ocena oparta na innych kryteriach pozostawia wątpliwości co do stosowności administracyjnej kary pieniężnej zarówno jako samodzielnego środka naprawczego, lub też w połączeniu z innymi środkami na mocy art. 58, owe obciążające lub łagodzące okoliczności mogą pomóc organowi nadzorczemu w dokonaniu wyboru odpowiednich środków, przechylając szalę na korzyść tego, co w danym przypadku okazuje się bardziej skuteczne, proporcjonalne i odstraszające.

Przepis ten ma na celu oszacowanie stopnia odpowiedzialności administratora po wystąpieniu naruszenia. Może on obejmować przypadki, w których administrator / podmiot przetwarzający wyraźnie nie wykazali się lekkomyślną/lekceważącą postawą, ale po stwierdzeniu naruszenia dołożyli wszelkich starań, by naprawić skutki swoich działań.

Wcześniejsze doświadczenia regulacyjne organów nadzorczych ze stosowania dyrektywy 95/46/WE dowiodły, że właściwe może być wykazanie się pewną elastycznością wobec administratorów danych / podmiotów przetwarzających, którzy przyznali się do naruszenia i podjęli działania zmierzające do naprawy lub ograniczenia skutku swoich działań. Działania takie mogą obejmować (choć nie muszą prowadzić do większej elastyczności w każdym przypadku):

- kontaktowanie się z innymi administratorami / podmiotami przetwarzającymi, którzy mogli uczestniczyć w rozszerzeniu zakresu przetwarzania, np. w przypadku gdy doszło do omyłkowego udostępnienia danych stronom trzecim.
- działania podjęte we właściwym czasie przez administratora / podmiot przetwarzający w celu powstrzymania naruszenia lub jego dalszego rozwoju do poziomu lub etapu, na którym owo naruszenie stałoby się znacznie poważniejsze niż pierwotnie.

d) Stopień odpowiedzialności administratora lub podmiotu przetwarzającego z uwzględnieniem środków technicznych i organizacyjnych wdrożonych przez nich na mocy art. 25 i 32

Rozporządzenie wprowadziło znacznie wyższy poziom rozliczalności administratora danych w porównaniu z dyrektywą o ochronie danych 95/46/WE.

Stopień odpowiedzialności administratora lub podmiotu przetwarzającego oceniany w kontekście stosowania odpowiedniego środka naprawczego może obejmować następujące kwestie:

- Czy administrator wdrożył środki techniczne zgodne z zasadą uwzględniania ochrony danych w fazie projektowania lub z zasadą domyślnej ochrony danych (art. 25)?
- Czy administrator wdrożył środki organizacyjne, które zapewniają skuteczność zasady uwzględniania ochrony danych w fazie projektowania i zasady domyślnej ochrony danych (art. 25) na wszystkich poziomach organizacji?
- Czy administrator / podmiot przetwarzający zapewnił odpowiedni poziom bezpieczeństwa (art. 32)?
- Czy na odpowiednim poziomie zarządzania w organizacji są znane i stosowane właściwe procedury/polityki ochrony danych (art. 24)?

Przepisy art. 25 i 32 rozporządzenia wymagają, by administratorzy „*uwzględnili stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania*". Zamiast ustanowienia obowiązku celu, przepisy te

wprowadzają raczej obowiązek zapewnienia środków, tzn. administrator musi dokonać niezbędnych ocen i wyciągnąć odpowiednie wnioski. Następnie organ nadzorczy musi odpowiedzieć na pytanie, w jakim stopniu administrator „zrobił wszystko, czego można by było oczekiwać", zważywszy na charakter, cele lub zakres przetwarzania oraz w świetle obowiązków nałożonych na niego przez rozporządzenie.

W ocenie tej należy odpowiednio uwzględnić wszelkie sposoby postępowania lub metody opierające się na „najlepszych praktykach", jeżeli takie istnieją i mają zastosowanie. Należy wziąć pod uwagę normy branżowe, a także kodeksy postępowania w danej dziedzinie lub zawodzie. Kodeksy postępowania mogą wskazywać na to, co jest powszechną praktyką w danej dziedzinie, oraz jaki jest poziom wiedzy na temat różnych środków rozwiązywania typowych problemów bezpieczeństwa związanych z przetwarzaniem.

Chociaż zwykle idealnym działaniem jest naśladowanie najlepszych praktyk, to przy dokonywaniu oceny stopnia odpowiedzialności należy brać pod uwagę szczególne okoliczności danej sprawy.

e) Wszelkie istotne wcześniejsze naruszenia, których dopuścił się administrator lub podmiot przetwarzający

To kryterium ma na celu ocenę dotychczasowego przebiegu działalności podmiotu dopuszczającego się naruszenia. Organy nadzorcze powinny wziąć pod uwagę fakt, że zakres takiej oceny może być dość szeroki, gdyż każdy rodzaj naruszenia rozporządzenia, nawet jeśli jest inny niż ten, który jest obecnie badany przez organ nadzorczy, może być „istotny" dla oceny, ponieważ mógłby wskazywać na ogólny poziom niewystarczającej wiedzy lub lekceważenie zasad ochrony danych.

Organ nadzorczy powinien ocenić:

- Czy administrator / podmiot przetwarzający dopuścił się wcześniej tego samego naruszenia?
- Czy administrator / podmiot przetwarzający dopuścił się naruszenia rozporządzenia w ten sam sposób? (np. w wyniku niewystarczającej znajomości istniejących procedur w organizacji lub w wyniku niewłaściwej oceny ryzyka, braku reakcji na wnioski osób, których dane dotyczą, w odpowiednim czasie, nieuzasadnionego opóźnienia w udzielaniu odpowiedzi na wnioski itp.).

f) Stopień współpracy z organem nadzorczym w celu usunięcia naruszenia oraz złagodzenia jego ewentualnych negatywnych skutków

Artykuł 83 ust. 2 stanowi, że należy zwrócić „należytą uwagę" na stopień współpracy podczas podejmowania decyzji na temat ewentualnego nałożenia administracyjnej kary pieniężnej oraz ustalenia jej wysokości. Rozporządzenie nie zawiera precyzyjnej odpowiedzi na pytanie, w jaki sposób uwzględnić starania administratorów lub podmiotów przetwarzających na rzecz usunięcia naruszenia wykrytego przez organ nadzorczy. Ponadto oczywiste jest, że kryteria te stosuje się zwykle przy ustalaniu wysokości kary pieniężnej, jaka zostanie nałożona.

Jednakże w przypadku gdy interwencja administratora spowodowała brak negatywnych konsekwencji dla praw danych osób lub bardziej ograniczony wpływ tych konsekwencji niż mogłoby to mieć miejsce, można to również uwzględnić przy wyborze środka naprawczego, który będzie proporcjonalny w konkretnej sprawie.

Jednym z przykładów sprawy, w którym warto rozważyć współpracę z organem nadzorczym, może być następująca sytuacja:

- Czy podmiot zareagował w określony sposób na wnioski organu nadzorczego w fazie dochodzenia w tej konkretnej sprawie, co w rezultacie znacznie ograniczyło wpływ na prawa danych osób?

Należy równocześnie zaznaczyć, że niestosowne byłoby dodatkowe podnoszenie kwestii współpracy, która jest już wymagana przepisami prawa, np. podmiot jest zobowiązany w każdym przypadku do zapewnienia organowi nadzorczemu dostępu do pomieszczeń w celu przeprowadzenia audytów/inspekcji.

g) Kategorie danych osobowych, których dotyczyło naruszenie

Oto kilka przykładów kluczowych pytań, na które organ nadzorczy — w stosownych przypadkach — może uznać za konieczne udzielić odpowiedzi:

- Czy naruszenie dotyczy przetwarzania szczególnych kategorii danych określonych w art. 9 lub 10 rozporządzenia?
- Czy dane są bezpośrednio/pośrednio możliwe do zidentyfikowania?
- Czy przetwarzanie obejmuje dane, których rozpowszechnienie natychmiast spowodowałoby szkodę/dyskomfort danej osoby (leżące poza zakresem kategorii określonych w art. 9 lub 10)?

- Czy dane są dostępne bezpośrednio bez zabezpieczeń technicznych, czy też są zaszyfrowane[13]?

h) Sposób, w jaki organ nadzorczy dowiedział się o naruszeniu — w szczególności czy i w jakim zakresie administrator lub podmiot przetwarzający zgłosił naruszenie

Organ nadzorczy może dowiedzieć się o naruszeniu w wyniku postępowania, skarg, artykułów w prasie, anonimowych wskazówek lub powiadomienia przez administratora danych. Zgodnie z rozporządzeniem administrator ma obowiązek zawiadomić organ nadzorczy o naruszeniu ochrony danych osobowych. Zwykle dopełnienie tego obowiązku przez administratora nie może być interpretowane jako czynnik osłabiający/łagodzący. Podobnie administrator / podmiot przetwarzający, który wykazał się niedbałością, gdyż nie dopełnił obowiązku powiadomienia lub co najmniej nie powiadomił o wszystkich szczegółach naruszenia wskutek niepoprawnej oceny rozmiaru naruszenia, może według organu nadzorczego zasłużyć na poważniejszą sankcję — innymi słowy jest mało prawdopodobne, by takie naruszenie zostało uznane za niewielkie.

i) Jeżeli wobec administratora lub podmiotu przetwarzającego, których sprawa dotyczy, zostały wcześniej zastosowane w tej samej sprawie środki, o których mowa w art. 58 ust. 2 — przestrzeganie tych środków

Po wykryciu wcześniejszego naruszenia administrator lub podmiot przetwarzający mogli być monitorowani przez organ nadzorczy pod kątem przestrzegania tych środków, natomiast do kontaktów z inspektorem ochrony danych, jeśli takowe istniały, prawdopodobnie dochodziło wielokrotnie. Z tego powodu organ nadzorczy uwzględni wcześniejsze kontakty.

W przeciwieństwie do kryteriów określonych w lit. e) niniejsze kryteria oceny mają jedynie na celu przypomnienie organom nadzorczym, by stosowały środki, które same uprzednio wydały wobec tego samego administratora lub podmiotu przetwarzającego „*w tej samej sprawie*".

j) Stosowanie zatwierdzonych kodeksów postępowania na mocy art. 40 lub zatwierdzonych mechanizmów certyfikacji na mocy art. 42

Organy nadzorcze mają obowiązek „*monitorować i egzekwować stosowanie niniejszego rozporządzenia*" (art. 57 ust. 1 lit. a)). Administrator lub podmiot przetwarzający mogą wykazać wywiązywanie się z ciążących na nich obowiązków poprzez stosowanie zatwierdzonych kodeksów postępowania zgodnie z art. 24 ust. 3, art. 28 ust. 5 lub art. 32 ust. 3.

W przypadku naruszenia jednego z przepisów rozporządzenia stosowanie zatwierdzonego kodeksu postępowania może wskazywać na kompleksowość potrzeby interweniowania za pomocą skutecznej, proporcjonalnej i odstraszającej administracyjnej kary pieniężnej lub innego środka naprawczego wyznaczonego przez organ nadzorczy. Zgodnie z art. 40 ust. 4 zatwierdzone kodeksy postępowania przewidują „*mechanizmy pozwalające (monitorującemu) podmiotowi prowadzić obowiązkowe monitorowanie przestrzegania przepisów kodeksu*".

W przypadku gdy administrator lub podmiot przetwarzający zastosował się do zatwierdzonego kodeksu postępowania, organ nadzorczy może być przekonany, że społeczność stosująca kodeks odpowiedzialna za zarządzanie kodeksem sama podejmie odpowiednie działania przeciwko swojemu członkowi, np. za pomocą systemów monitorowania i egzekwowania kodeksu postępowania. Zatem organ nadzorczy może uznać, że takie środki są wystarczająco skuteczne, proporcjonalne lub odstraszające w danym przypadku, bez konieczności nakładania dodatkowych środków przez sam

[13] Nie zawsze należy uważać za „bonusowy" czynnik łagodzący to, że naruszenie dotyczy wyłącznie pośrednio możliwych do zidentyfikowania lub nawet spseudonimizowanych/zaszyfrowanych danych. W przypadku takich naruszeń ogólna ocena pozostałych kryteriów może w sposób umiarkowany lub zdecydowany zasugerować nałożenie kary pieniężnej.

organ nadzorczy. Pewne formy karania niezgodnego z przepisami zachowania można wprowadzić za pomocą schematu monitorowania, zgodnie z art. 41 ust. 2 lit. c) i art. 41 ust. 4, np. poprzez zawieszenie lub wykluczenie administratora lub podmiot przetwarzający spośród stosujących kodeks. Niemniej jednak uprawnienia organu monitorującego pozostają *„bez uszczerbku dla zadań i uprawnień właściwego organu nadzorczego*", innymi słowy organ nadzorczy nie ma obowiązku uwzględnienia wcześniej nałożonych kar dotyczących systemu samoregulacyjnego.

Niestosowanie środków samoregulacyjnych może również ujawniać zaniedbanie administratora / podmiotu przetwarzającego lub umyślne niestosowanie tych środków.

k) Wszelkie inne obciążające lub łagodzące czynniki mające zastosowanie do okoliczności sprawy, takie jak osiągnięte bezpośrednio lub pośrednio w związku z naruszeniem korzyści finansowe lub uniknięte straty

Sam przepis zawiera przykłady innych elementów, które można uwzględniać przy podejmowaniu decyzji co do stosowności administracyjnej kary pieniężnej nałożonej za naruszenie przepisów, o których mowa w art. 83 ust. 4–6.

Informacje na temat korzyści finansowych uzyskanych w wyniku naruszenia mogą być szczególnie istotne dla organów nadzorczych, gdyż takie korzyści nie mogą być rekompensowane za pomocą środków, które nie mają charakteru pieniężnego. W związku z tym fakt, że administrator osiągnął korzyści z tytułu naruszenia rozporządzenia może stanowić wyraźną przesłankę do zastosowania kary pieniężnej.

IV. Wniosek

Rozważania dotyczące kwestii takich jak te, o których mowa była w poprzedniej sekcji, umożliwią organom nadzorczym zidentyfikowanie — na podstawie odpowiednich okoliczności faktycznych sprawy — kryteriów, które są najbardziej przydatne przy podejmowaniu decyzji dotyczącej ewentualnego nałożenia, oprócz lub zamiast innych środków na mocy art. 58, odpowiedniej administracyjnej kary pieniężnej. Biorąc pod uwagę kontekst takiej oceny, organ nadzorczy określi najbardziej skuteczny, proporcjonalny i odstraszający środek naprawczy w celu zaradzenia naruszeniu.

Artykuł 58 zawiera wytyczne dotyczące rodzaju środków, które organ nadzorczy może zastosować, gdyż same środki naprawcze mają różny charakter i są dostosowane przede wszystkim do osiągnięcia różnych celów. Niektóre ze środków opisanych w art. 58 można nawet łączyć, osiągając tym samym działanie regulacyjne obejmujące więcej niż jeden środek naprawczy.

Nie zawsze jest konieczne uzupełnienie środka innym środkiem naprawczym. Na przykład: Skuteczność i odstraszający charakter interwencji organu nadzorczego przy należytym uwzględnieniu tego, co jest proporcjonalne do tego konkretnego przypadku, można osiągnąć wyłącznie za pomocą kary pieniężnej.

Krótko mówiąc, organy muszą przywrócić zgodność za pomocą wszystkich dostępnych im środków naprawczych. Organy nadzorcze będą miały również obowiązek dokonać wyboru najwłaściwszego sposobu wdrożenia działań regulacyjnych. Przykładowo takim sposobem może być nałożenie sankcji karnych (jeżeli są one dostępne na poziomie krajowym).

Konsekwentne stosowanie administracyjnych kar pieniężnych w całej Unii Europejskiej to rozwijająca się praktyka. Współpracujące ze sobą organy nadzorcze winny podejmować działania zmierzające do ciągłego zapewniania większej spójności w stosowaniu tych kar. Można to osiągnąć dzięki regularnej wymianie doświadczeń w ramach warsztatów szkoleniowych poświęconych rozpatrywaniu spraw lub innym wydarzeniom, które umożliwią porównanie spraw ze szczebla niższego niż krajowy, krajowego i transgranicznego. Zaleca się utworzenie stałej podgrupy powiązanej z odpowiednią częścią Europejskiej Rady Ochrony Danych w celu wspierania tej bieżącej działalności.

GRUPA ROBOCZA ART. 29

17/PL

WP 248 rev.01

Wytyczne dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko" do celów rozporządzenia 2016/679

Przyjęte w dniu 4 kwietnia 2017 r.

Ostatnio zmienione i przyjęte w dniu 4 października 2017 r.

Grupa Robocza została powołana na mocy art. 29 dyrektywy 95/46/WE. Jest ona niezależnym europejskim organem doradczym w zakresie ochrony danych i prywatności. Zadania Grupy zostały określone w przepisach art. 30 dyrektywy 95/46/WE i art. 15 dyrektywy 2002/58/WE.

Obsługę sekretariatu zapewnia Dyrekcja C (Prawa Podstawowe i Obywatelstwo Unii Europejskiej) Dyrekcji Generalnej ds. Sprawiedliwości, B-1049 Bruksela, Belgia, biuro nr MO-59 03/075.

Strona internetowa: http://ec.europa.eu/justice/data-protection/index_en.htm

GRUPA ROBOCZA DS. OCHRONY OSÓB FIZYCZNYCH W ZAKRESIE PRZETWARZANIA DANYCH OSOBOWYCH

powołana na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r.,

uwzględniając art. 29 i 30 tej dyrektywy,

uwzględniając swój regulamin wewnętrzny,

PRZYJMUJE NINIEJSZE WYTYCZNE:

Spis treści

I. WPROWADZENIE 5

II. ZAKRES WYTYCZNYCH 6

III. OCENA SKUTKÓW DLA OCHRONY DANYCH: WYJAŚNIENIA PRZEPISÓW ROZPORZĄDZENIA 8

A. CZEGO DOTYCZY OCENA SKUTKÓW DLA OCHRONY DANYCH? POJEDYNCZA OPERACJA PRZETWARZANIA LUB ZBIÓR PODOBNYCH OPERACJI PRZETWARZANIA 9

B. KTÓRE OPERACJE PRZETWARZANIA PODLEGAJĄ OCENIE SKUTKÓW DLA OCHRONY DANYCH? Z WYJĄTKIEM OPERACJI, KTÓRE „MOGĄ POWODOWAĆ WYSOKIE RYZYKO". 10

a) Kiedy przeprowadzenie oceny skutków dla ochrony danych jest obowiązkowe? Gdy przetwarzanie „może powodować wysokie ryzyko". 10

b) Kiedy przeprowadzenie oceny skutków dla ochrony danych nie jest obowiązkowe? W przypadku, gdy nie jest prawdopodobne, aby operacja przetwarzania „mogła powodować wysokie ryzyko", gdy przeprowadzono już podobną ocenę skutków dla ochrony danych, gdy operację zatwierdzono przed majem 2018 r., lub gdy posiada podstawę prawną lub znajduje się w wykazie operacji przetwarzania, które nie podlegają ocenie skutków dla ochrony danych. 16

C. A CO Z JUŻ ISTNIEJĄCYMI OPERACJAMI PRZETWARZANIA? W PEWNYCH OKOLICZNOŚCIACH WYMAGANE JEST PRZEPROWADZENIE OCEN SKUTKÓW DLA OCHRONY DANYCH. 17

D. JAK PRZEPROWADZIĆ OCENĘ SKUTKÓW DLA OCHRONY DANYCH? 18

a) W jakim momencie należy przeprowadzić ocenę skutków dla ochrony danych? Przed rozpoczęciem przetwarzania. 18

b) Kto jest zobowiązany do przeprowadzenia oceny skutków dla ochrony danych? Administrator, wspólnie z DPO i podmiotem przetwarzającym. 18

c) Zgodnie z jaką metodyką przeprowadza się ocenę skutków dla ochrony danych? Różna metodyka, wspólne kryteria. 20

d) Czy publikacja oceny skutków dla ochrony danych jest obowiązkowa? Nie, lecz publikacja podsumowania może przyczynić się do zwiększenia zaufania, a pełną treść oceny skutków dla ochrony danych należy przekazać organom nadzorczym, jeżeli miały miejsce uprzednie konsultacje lub jeżeli zwrócił się o to organ ochrony danych. 23

E. KIEDY NALEŻY SKONSULTOWAĆ SIĘ Z ORGANEM NADZORCZYM? JEŻELI RYZYKO SZCZĄTKOWE JEST WYSOKIE. 24

IV. WNIOSKI I ZALECENIA 25

ZAŁĄCZNIK 1 – PRZYKŁADY ISTNIEJĄCYCH UNIJNYCH RAM DOKONYWANIA OCENY SKUTKÓW DLA OCHRONY DANYCH 27

ZAŁĄCZNIK 2 – KRYTERIA DOPUSZCZALNEJ OCENY SKUTKÓW DLA OCHRONY DANYCH 29

I. Wprowadzenie

Rozporządzenie 2016/679[1] (RODO) będzie obowiązywało od dnia 25 maja 2018 r. W art. 35 RODO – podobnie jak w dyrektywie 2016/680[2]– wprowadzono pojęcie oceny skutków dla ochrony danych[3].

Ocena skutków dla ochrony danych jest procesem pozwalającym opisać przetwarzanie oraz ocenić jego konieczność i proporcjonalność, a także mającym wspomóc zarządzanie ryzykiem naruszenia praw i wolności osób fizycznych wynikającym z przetwarzania danych osobowych[4] poprzez ocenę ryzyka i określenie środków pozwalającym zaradzić tym czynnikom ryzyka. Oceny skutków dla ochrony danych są ważnym narzędziem rozliczalności, ponieważ ułatwiają administratorom nie tylko przestrzeganie wymogów określonych w RODO, ale także wykazanie, że podjęto odpowiednie środki w celu zapewnienia przestrzegania przepisów RODO (zob. również art. 24)[5]. Innymi słowy **ocena skutków dla ochrony danych jest procesem budowania i wykazywania zgodności**.

Na mocy RODO nieprzestrzeganie wymogów dotyczących oceny skutków dla ochrony danych może spowodować nałożenie grzywien przez właściwy organ nadzorczy. Nieprzeprowadzenie oceny skutków dla ochrony danych, gdy przetwarzanie podlega takiej ocenie (art. 35 ust. 1 i 3–4), nieprawidłowe przeprowadzenie oceny skutków dla ochrony danych (art. 35 ust. 2 i 7–9) lub brak

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

[2] W innych kontekstach w odniesieniu do tej samej koncepcji często stosuje się pojęcie „ocena skutków w zakresie prywatności".

[3] Art. 27 dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych stanowi również, że ocena skutków w zakresie prywatności jest potrzebna, ponieważ „przetwarzanie [...] może skutkować powstaniem wysokiego ryzyka naruszenia praw i wolności osób fizycznych".

[4] RODO nie zawiera jako takiej formalnej definicji pojęcia „ocena skutków dla ochrony danych", ale

- w art. 35 ust. 7 sprecyzowano, że ocena powinna zawierać co najmniej:
  - „a) systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez administratora;
  - b) ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;
  - c) ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą, o którym mowa w ust. 1; oraz
  - d) środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie niniejszego rozporządzenia, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy";
- jego znaczenie i rolę wyjaśniono w motywie 84 w następujący sposób: „aby poprawić przestrzeganie niniejszego rozporządzenia, gdy operacje przetwarzania mogą wiązać się z wysokim ryzykiem naruszenia praw lub wolności osób fizycznych, należy zobowiązać administratora do dokonania oceny skutków dla ochrony danych w celu oszacowania w szczególności źródła, charakteru, specyfiki i powagi tego ryzyka".

[5] Zob. również motyw 84: „wyniki oceny należy uwzględnić przy określaniu odpowiednich środków, które należy zastosować, by wykazać, że przetwarzanie danych osobowych odbywa się zgodnie z niniejszym rozporządzeniem".

konsultacji z właściwym organem nadzorczym, gdy jest to wymagane (art. 36 ust. 3 lit. e)) mogą skutkować nałożeniem administracyjnej kary pieniężnej w wysokości do 10 mln EUR lub, w przypadku przedsiębiorstwa, do 2 % całkowitego rocznego obrotu w skali światowej w poprzednim roku budżetowym, w zależności od tego, która kwota jest wyższa.

II. Zakres wytycznych

W niniejszych wytycznych uwzględniono:

- oświadczenie 14/EN WP 218 Grupy Roboczej Art. 29[6];
- wytyczne Grupy Roboczej Art. 29 dotyczące inspektora ochrony danych 16/EN WP 243[7];
- opinię Grupy Roboczej Art. 29 w sprawie ograniczenia celu 13/EN WP 203[8];
- normy międzynarodowe[9].

Zgodnie z przewidzianym w RODO podejściem opartym na analizie ryzyka przeprowadzenie oceny skutków dla ochrony danych nie jest obowiązkowe w przypadku każdej operacji przetwarzania. Przeprowadzenia oceny skutków dla ochrony danych wymaga się wyłącznie w przypadku, gdy przetwarzanie „może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych" (art. 35 ust. 1). Aby zapewnić spójną interpretację okoliczności, w których ocena skutków dla ochrony danych jest obowiązkowa (art. 35 ust. 3), niniejsze wytyczne mają na celu przede wszystkim wyjaśnienie tego pojęcia i przedstawienie kryteriów w odniesieniu do wykazów, które zostaną przyjęte przez organy ochrony danych zgodnie z art. 35 ust. 4.

Zgodnie z art. 70 ust. 1 lit. e) Europejska Rada Ochrony Danych będzie mogła wydawać wytyczne, zalecenia i najlepsze praktyki, zachęcając do spójnego stosowania RODO. Celem niniejszego dokumentu jest uprzedzenie takich przyszłych prac Europejskiej Rady Ochrony Danych i tym samym objaśnienie odpowiednich przepisów RODO, aby pomóc administratorom w przestrzeganiu prawa oraz aby zapewnić pewność prawa administratorom, którzy są zobowiązani do przeprowadzenia oceny skutków dla ochrony danych.

Niniejsze wytyczne mają na celu również promowanie opracowania:

- wspólnego unijnego wykazu operacji przetwarzania, w przypadku których ocena skutków dla ochrony danych jest obowiązkowa (art. 35 ust. 4);

[6] oświadczenie 14/EN WP 218 Grupy Roboczej Art. 29 dotyczące roli opartego na analizie ryzyka podejścia do ram prawnych w zakresie ochrony danych przyjęte w dniu 30 maja 2014 r. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf?wb48617274=72C54532

[7] Wytyczne Grupy Roboczej Art. 29 dotyczące inspektora ochrony danych 16/EN WP 243 przyjęte w dniu 13 grudnia 2016 r. http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf?wb48617274=CD63BD9A

[8] Opinia Grupy Roboczej Art. 29 nr 03/2013 w sprawie ograniczenia celu 13/EN WP 203 przyjęta w dniu 2 kwietnia 2013 r. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf?wb48617274=39E0E409

[9] Np. ISO 31000:2009, Zarządzanie ryzykiem – Zasady i wytyczne, Międzynarodowa Organizacja Normalizacyjna (ISO); ISO/IEC 29134 (projekt), IT – Techniki bezpieczeństwa – ocena skutków w zakresie prywatności – Wytyczne, Międzynarodowa Organizacja Normalizacyjna (ISO).

- wspólnego unijnego wykazu operacji przetwarzania, w przypadku których ocena skutków dla ochrony danych nie jest konieczna (art. 35 ust. 5);
- wspólnych kryteriów dotyczących metody przeprowadzania oceny skutków dla ochrony danych (art. 35 ust. 5);
- wspólnych kryteriów dotyczących określania, kiedy należy skonsultować się z organem nadzorczym (art. 36 ust. 1);
- w stosownych przypadkach – zaleceń bazujących na doświadczeniach zgromadzonych w państwach członkowskich UE.

III. Ocena skutków dla ochrony danych: wyjaśnienia przepisów rozporządzenia

W RODO na administratorów nakłada się obowiązek wdrożenia odpowiednich środków pozwalających zapewnić przestrzeganie przepisów RODO oraz możliwość wykazania przestrzegania tych przepisów, uwzględniając m.in. „ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia" (art. 24 ust. 1). Obowiązek przeprowadzania przez administratorów oceny skutków dla ochrony danych w określonych okolicznościach należy rozumieć w kontekście ich ogólnego obowiązku, jakim jest właściwe zarządzanie ryzykiem[10] związanym z przetwarzaniem danych osobowych.

„Ryzyko" jest scenariuszem opisującym zdarzenie i jego konsekwencje, oszacowanym pod względem powagi i prawdopodobieństwa ryzyka. „Zarządzanie ryzykiem" można natomiast zdefiniować jako skoordynowane działania mające na celu kierowanie organizacją i kontrolowanie organizacji pod względem ryzyka.

W art. 35 odniesiono się do prawdopodobnego wysokiego ryzyka „naruszenia praw lub wolności osób fizycznych". Jak wskazano w oświadczeniu Grupy Roboczej Art. 29 dotyczącym roli opartego na analizie ryzyka podejścia do ram prawnych w zakresie ochrony danych, odniesienie do „praw i wolności" osób, których dane dotyczą, dotyczy przede wszystkim prawa do ochrony danych i prywatności, ale może również obejmować inne prawa podstawowe, takie jak wolność słowa, wolność myśli, swoboda poruszania się, zakaz dyskryminacji, prawo do wolności, wolność sumienia i wolność religii.

Zgodnie z przewidzianym w RODO podejściem opartym na analizie ryzyka przeprowadzenie oceny skutków dla ochrony danych nie jest obowiązkowe w przypadku każdej operacji przetwarzania. Przeprowadzenia oceny skutków dla ochrony danych wymaga się natomiast wyłącznie w przypadku, gdy dany rodzaj przetwarzania „może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych" (art. 35 ust. 1). Sam fakt niespełnienia warunków nakładających obowiązek przeprowadzenia oceny skutków dla ochrony danych nie zmniejsza jednak ogólnego obowiązku wdrożenia przez administratorów środków umożliwiających odpowiednie zarządzanie ryzykiem naruszenia prawa i wolności osób, których dane dotyczą. W praktyce oznacza to, że administratorzy muszą stale oceniać ryzyko powodowane przez czynności przetwarzania w celu określenia, kiedy dany rodzaj przetwarzania „może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych".

[10] Należy podkreślić, że aby być w stanie zarządzać ryzykiem naruszenia praw i wolności osób fizycznych, ryzyko to należy określić, przeanalizować, oszacować, ocenić, wyeliminować (np. złagodzić...) oraz poddawać regularnym przeglądom. Administratorzy nie mogą uniknąć odpowiedzialności, zawierając umowy ubezpieczeniowe na wypadek danego ryzyka.

Na poniższym wykresie przedstawiono podstawowe zasady związane z oceną skutków dla ochrony danych, o których mowa w RODO:



A. Czego dotyczy ocena skutków dla ochrony danych? Pojedyncza operacja przetwarzania lub zbiór podobnych operacji przetwarzania.

Ocena skutków dla ochrony danych może dotyczyć pojedynczej operacji przetwarzania danych. Art. 35 ust. 1 stanowi jednak, że „dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę". W motywie 92 dodaje się, że „w niektórych okolicznościach rozsądnie i korzystnie byłoby nie ograniczać oceny skutków dla ochrony danych do pojedynczego projektu, na przykład w przypadkach gdy organy lub podmioty publiczne zamierzają ustanowić wspólną aplikację lub platformę przetwarzania lub gdy kilku administratorów planuje wprowadzić wspólną aplikację lub środowisko przetwarzania obejmujące sektor lub segment gospodarki lub szeroko rozpowszechnioną działalność horyzontalną".

Do oceny wielu operacji przetwarzania, które są podobne pod względem charakteru, zakresu, kontekstu, celu i ryzyka **można wykorzystać jedną ocenę skutków dla ochrony danych**. Celem ocen skutków dla ochrony danych jest bowiem systematyczne analizowanie nowych sytuacji, które mogłyby prowadzić do wysokiego ryzyka naruszenia praw i wolności osób fizycznych, dlatego nie ma potrzeby przeprowadzania oceny skutków dla ochrony danych (tj. operacji przetwarzania przeprowadzonych w określonym kontekście i w konkretnym celu) w przypadkach, które zostały już przeanalizowane. Może to mieć miejsce w przypadku wykorzystania podobnej technologii do gromadzenia tego samego rodzaju danych do tych samych celów. Na przykład grupa władz miejskich, które instalują podobny system CCTV, może przeprowadzić pojedynczą ocenę skutków dla ochrony danych obejmującą przetwarzanie danych przez oddzielnych administratorów; lub podmiot w branży kolejowej (pojedynczy administrator) może zainstalować nadzór wideo na wszystkich stacjach kolejowych w ramach jednej oceny skutków dla ochrony danych. Może to również dotyczyć podobnych operacji przetwarzania prowadzonych przez różnych administratorów danych. W takich przypadkach należy udostępniać lub upubliczniać referencyjną ocenę skutków dla ochrony danych, wdrożyć środki opisane w ocenie skutków dla ochrony danych oraz przedstawić uzasadnienie przeprowadzenia pojedynczej oceny skutków dla ochrony danych.

Jeżeli operacja przetwarzania obejmuje współadministratorów, muszą oni dokładnie określić swoje obowiązki. W swojej ocenie skutków dla ochrony danych administratorzy powinni określić, która strona ponosi odpowiedzialność za poszczególne środki mające na celu wyeliminowanie ryzyka oraz za ochronę praw i wolności osób, których dane dotyczą. Każdy administrator danych powinien wyrazić swoje potrzeby i dzielić się przydatnymi informacjami bez ujawniania tajemnic (np.: ochrona tajemnicy przedsiębiorstwa, własności intelektualnej, poufnych informacji handlowych) albo słabych stron.

Ocena skutków dla ochrony danych może być również przydatna do oceny skutków dla ochrony danych wywieranych przez dany produkt technologiczny, np. sprzęt lub oprogramowanie, gdy istnieje prawdopodobieństwo, że różni administratorzy danych będą korzystać z niego do przeprowadzania różnych operacji przetwarzania. Oczywiście administrator danych wdrażający produkt nadal jest zobowiązany do przeprowadzenia własnej oceny skutków dla ochrony danych w odniesieniu do tego konkretnego procesu wdrażania, ale w stosownych przypadkach może poinformować o tym fakcie za pomocą oceny skutków dla ochrony danych przygotowanej przez dostawcę produktu. Przykładem może być związek między producentami inteligentnych liczników a przedsiębiorstwami użyteczności publicznej. Każdy dostawca produktu lub podmiot przetwarzający powinien dzielić się przydatnymi informacjami bez ujawniania tajemnic i bez stwarzania zagrożeń dla bezpieczeństwa poprzez ujawnienie słabych stron.

B. Które operacje przetwarzania podlegają ocenie skutków dla ochrony danych? Z wyjątkiem operacji, które „mogą powodować wysokie ryzyko".

W niniejszej sekcji opisano sytuacje, w których przeprowadzenie oceny skutków dla ochrony danych jest obowiązkowe oraz sytuacje, w których nie jest to konieczne.

O ile operacja przetwarzania nie stanowi wyjątku (rozdział III sekcja B lit. a)), ocenę skutków dla ochrony danych należy przeprowadzić wówczas, gdy operacja przetwarzania „może powodować wysokie ryzyko" (rozdział III sekcja B lit. b)).

a) Kiedy przeprowadzenie oceny skutków dla ochrony danych jest obowiązkowe? Gdy przetwarzanie „może powodować wysokie ryzyko".

W RODO nie wymaga się przeprowadzenia oceny skutków dla ochrony danych w odniesieniu do każdej operacji przetwarzania, która może powodować ryzyko naruszenia praw i wolności osób fizycznych. Przeprowadzenie oceny skutków dla ochrony danych jest obowiązkowe wyłącznie w przypadku, gdy przetwarzanie „może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych" (art. 35 ust. 1 zilustrowany art. 35 ust. 3 i uzupełniony art. 35 ust. 4). Jest to szczególnie istotne przy wprowadzaniu nowej technologii przetwarzania danych[11].

W przypadkach, w których nie jest jasne, czy wymagane jest przeprowadzenie oceny skutków dla ochrony danych, Grupa Robocza Art. 29 zaleca jednak przeprowadzenie takiej oceny, ponieważ stanowi ona przydatne narzędzie ułatwiające administratorom przestrzeganie przepisów o ochronie danych.

[11] Więcej przykładów można znaleźć w motywach 89 i 91 oraz w art. 35 ust. 1 i 3.

Mimo że przeprowadzenie oceny skutków dla ochrony danych może być wymagane w innych okolicznościach, w art. 35 ust. 3 przedstawiono kilka przykładów, gdy operacja przetwarzania „może powodować wysokie ryzyko", w szczególności w przypadku:

- „a) systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną[12];
- b) przetwarzania na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1, lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10[13]; lub
- c) systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie".

Jak wskazuje wyrażenie „w szczególności" w zdaniu wprowadzającym w art. 35 ust. 3 RODO, wymienione przykłady nie stanowią wyczerpującego wykazu. Mogą występować operacje przetwarzania „wysokiego ryzyka", których nie uwzględniono w wykazie, lecz stwarzają równie wysokie ryzyko. Wspomniane operacje przetwarzania powinny również podlegać ocenom skutków dla ochrony danych. Z tego powodu kryteria przedstawione poniżej wykraczają niekiedy poza proste wyjaśnienie tego, co należy rozumieć przez trzy przykłady podane w art. 35 ust. 3 RODO.

W celu przedstawienia bardziej konkretnego zbioru operacji przetwarzania wymagających przeprowadzenia oceny skutków dla ochrony danych ze względu na ich nieodłączne wysokie ryzyko, uwzględniając poszczególne elementy art. 35 ust. 1 i art. 35 ust. 3 lit. a)–c), wykaz, który zostanie przyjęty na szczeblu krajowym na mocy art. 35 ust. 4, i motywy 71, 75 i 91 oraz inne wspomniane w RODO odniesienia do operacji przetwarzania, które „mogą powodować wysokie ryzyko"[14], należy wziąć pod uwagę dziewięć następujących kryteriów.

1. Ocena lub punktacja, w tym profilowanie i prognozowanie w szczególności na podstawie „aspektów dotyczących efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się osoby, której dane dotyczą" (motywy 71 i 91). Przykładem tego może być instytucja finansowa sprawdzająca swoich klientów w referencyjnej bazie danych kredytowych lub bazie danych w zakresie przeciwdziałania praniu pieniędzy i zwalczania finansowania terroryzmu lub w bazie danych zawierającej informacje o nadużyciach finansowych; przykładem może być również przedsiębiorstwo biotechnologiczne bezpośrednio oferujące konsumentom badania genetyczne w celu oceny i prognozowania ryzyka wystąpienia choroby lub zagrożeń dla zdrowia, a także przedsiębiorstwo tworzące profile zachowań lub profile marketingowe w oparciu o wykorzystanie lub nawigację na swojej stronie internetowej.
2. Automatyczne podejmowanie decyzji o skutku prawnym lub podobnie znaczącym skutku: przetwarzanie mające na celu podjęcie decyzji w sprawie osób, których dane dotyczą,

[12] Zob. motyw 71: „w szczególności analizowane lub prognozowane aspekty dotyczące efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się – w celu tworzenia lub wykorzystywania profili osobistych".

[13] Zob. motyw 75: „jeżeli przetwarzane są dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, wyznanie lub przekonania światopoglądowe, lub przynależność do związków zawodowych oraz jeżeli przetwarzane są dane genetyczne, dane dotyczące zdrowia lub dane dotyczące seksualności lub wyroków skazujących i naruszeń prawa lub związanych z tym środków bezpieczeństwa".

[14] Zob. np. motywy 75, 76, 92, 116.

wywołujących „skutki prawne wobec osoby fizycznej" lub decyzji, które „w podobny sposób istotnie na nią wpływają" (art. 35 ust. 3 lit. a)). Przykładowo przetwarzanie może prowadzić do wykluczenia lub dyskryminacji osób fizycznych. Przetwarzanie mające niewielki wpływ na osoby fizyczne lub niemające na nie żadnego wpływu nie spełnia tego konkretnego kryterium. Dalsze wyjaśnienia dotyczące tych pojęć zostaną przedstawione w przyszłych wytycznych Grupy Roboczej Art. 29 dotyczących profilowania.

3. Systematyczne monitorowanie: przetwarzanie wykorzystywane do obserwacji, monitorowania lub kontrolowania osób, których dane dotyczą, w tym danych gromadzonych za pośrednictwem sieci lub ramach „systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie" (art. 35 ust. 3 lit. c))[15]. Ten rodzaj monitorowania stanowi jedno z kryteriów, ponieważ dane osobowe mogą być gromadzone w sytuacji, gdy osoby, których dane dotyczą, nie są świadome tego, kto gromadzi ich dane i w jaki sposób z nich korzysta. Ponadto osoby fizyczne mogą nie być w stanie uniknąć takiego rodzaju przetwarzania w przestrzeni publicznej (lub przestrzeni publicznie dostępnej).
4. Dane wrażliwe lub dane o charakterze wysoce osobistym: obejmują szczególne kategorie danych osobowych określone w art. 9 (np. informacje o poglądach politycznych obywateli) oraz dane osobowe dotyczące wyroków skazujących za przestępstwo lub naruszeń prawa zdefiniowane w art. 10. Przykładem może być szpital przechowujący dokumentację medyczną pacjentów lub prywatny detektyw przechowujący szczegółowe dane przestępców. Oprócz tych przepisów zawartych w RODO niektóre kategorie danych można uznać za zwiększające potencjalne ryzyko naruszenia praw i wolności osób fizycznych. Te dane osobowe uznaje się za szczególnie wrażliwe (zgodnie z powszechnym rozumieniem tego terminu), ponieważ są powiązane z gospodarstwem domowym i działalnością prywatną (taką jak łączność elektroniczna, której poufność należy chronić) lub ponieważ wpływają na wykonanie prawa podstawowego (takie jak dane dotyczące lokalizacji, których gromadzenie jest sprzeczne ze swobodą poruszania się), lub ponieważ ich naruszenie ma wyraźny wpływ na codzienne życie osób, których dane dotyczą (takie jak dane finansowe, które mogą zostać wykorzystane do oszustw płatniczych). W tym względzie może mieć znaczenie fakt, czy dane zostały upublicznione przez osobę, której dane dotyczą, czy przez osoby trzecie. Okoliczność, że dane osobowe są publicznie dostępne, może być uznana za czynnik w ocenie, jeżeli zgodnie z założeniami dane te miały być dalej wykorzystywane do określonych celów. Kryterium to może również obejmować dane takie jak dokumenty osobiste, wiadomości e-mail, pamiętniki, notatki z e-czytników wyposażonych w funkcję notatnika oraz dane mające bardzo osobisty charakter zawarte w aplikacjach rejestrujących codzienną aktywność.
5. Dane przetwarzane na dużą skalę: w RODO nie zawarto definicji pojęcia „przetwarzanie na dużą skalę", choć w motywie 91 przedstawiono pewne wskazówki w tym zakresie. W każdym razie Grupa Robocza Art. 29 zaleca, aby przy ustalaniu, czy przetwarzanie danych odbywa się na dużą skalę, wziąć pod uwagę w szczególności następujące czynniki[16]:
   a. liczbę osób, których dane dotyczą – wyrażoną jako konkretna wartość albo jako odsetek populacji odniesienia;
   b. ilość danych lub zakres poszczególnych przetwarzanych pozycji danych;
   c. czas trwania lub trwałość czynności przetwarzania danych;
   d. zakres geograficzny czynności przetwarzania.
6. Dopasowywanie lub łączenie zbiorów danych np. pochodzących z co najmniej dwóch operacji przetwarzania danych przeprowadzonych w różnych celach lub przez różnych administratorów danych w sposób wykraczający poza uzasadnione oczekiwania osób, których dane dotyczą[17].
7. Dane dotyczące osób wymagających szczególnej opieki, których dane dotyczą (zob. motyw 75): przetwarzanie tego rodzaju danych stanowi jedno z kryteriów ze względu na zwiększoną nierównowagę sił między osobami, których dane dotyczą, a administratorem danych, co oznacza, że osoby fizyczne mogą mieć trudności z wyrażeniem zgody na przetwarzanie swoich danych lub z wyrażeniem sprzeciwu wobec ich przetwarzania, lub mogą mieć trudności z korzystaniem z przysługujących im praw. Do osób wymagających szczególnej opieki, których dane dotyczą, można zaliczyć dzieci (można je uznać za niezdolne do świadomego i przemyślanego sprzeciwienia się przetwarzaniu danych lub do wyrażenia zgody na przetwarzanie danych), pracowników, bardziej wrażliwe grupy społeczne wymagające szczególnej ochrony (osoby chore psychicznie, osoby ubiegające się o azyl lub osoby starsze, pacjenci itp.) oraz w każdą sytuację, gdy można stwierdzić brak równowagi między stanowiskiem osoby, której dane dotyczą, a stanowiskiem administratora.
8. Innowacyjne wykorzystanie lub stosowanie nowych rozwiązań technologicznych lub organizacyjnych, takich jak połączenie technologii rozpoznającej odcisk palca i twarz w celu poprawy fizycznej kontroli dostępu itd. W RODO (art. 35 ust. 1 i motywy 89 i 91) wyjaśniono, że wykorzystanie nowej technologii zdefiniowanej „zgodnie ze stanem wiedzy technicznej" (motyw 91) może sprawić, iż konieczne będzie przeprowadzenie oceny skutków dla ochrony danych. Wynika to z tego, że zastosowanie takiej technologii może wiązać się z nowymi formami gromadzenia i wykorzystania danych, co może stwarzać ryzyko naruszenia praw i wolności osób fizycznych. W istocie osobiste i społeczne skutki wprowadzenia nowej technologii mogą nie być znane. Ocena skutków dla ochrony danych pomoże administratorowi danych zrozumieć takie ryzyko i je wyeliminować. Na przykład niektóre aplikacje „internetu rzeczy" mogą mieć znaczący wpływ na codzienne życie i prywatność osób fizycznych; dlatego wymagane jest przeprowadzenie oceny skutków dla ochrony danych.
9. Gdy samo przetwarzanie „uniemożliwia osobom, których dane dotyczą, wykonywanie prawa lub korzystanie z usługi lub umowy" (art. 22 i motyw 91). Obejmuje to operacje przetwarzania, których celem jest umożliwienie osobom, których dane dotyczą, uzyskania dostępu do usługi lub zawarcia umowy, zmiana tego dostępu lub odmówienie dostępu. Przykładem tego jest sytuacja, w której bank sprawdza swoich klientów w referencyjnej bazie danych kredytowych, aby zdecydować, czy udzielić im kredytu.

[15] Grupa Robocza Art. 29 przypisuje wyrażeniu „systematycznie" jedno lub kilka z poniższych znaczeń (zob. wytyczne Grupy Roboczej Art. 29 dotyczące inspektora ochrony danych 16/EN WP 243):
- przeprowadzane w ramach określonego systemu;
- wcześniej zaplanowane, zorganizowane lub mające metodyczny charakter;
- odbywające się w ramach ogólnego planu gromadzenia danych;
- realizowane jako część strategii.

Grupa Robocza Art. 29 interpretuje „miejsca publicznie dostępne" jako miejsca otwarte dla każdego obywatela, np. plac, centrum handlowe, ulica, rynek, stacja kolejowa lub biblioteka publiczna.

[16] Zob. wytyczne Grupy Roboczej Art. 29 dotyczące inspektora ochrony danych 16/EN WP 243.

[17] Zob. wyjaśnienie zawarte w opinii Grupy Roboczej Art. 29 w sprawie ograniczenia celu 13/EN WP 203, s. 24.

W większości przypadków administrator danych może uznać, że przetwarzanie spełniające dwa kryteria będzie wymagało przeprowadzenia oceny skutków dla ochrony danych. Ogólnie rzecz biorąc, Grupa Robocza Art. 29 uważa, że im więcej kryteriów zostanie spełnionych w ramach przetwarzania, tym większe prawdopodobieństwo wystąpienia wysokiego ryzyka naruszenia praw i wolności osób, których dane dotyczą, i dlatego wymaga przeprowadzenia oceny skutków dla ochrony danych, niezależnie od środków, jakie zamierza przyjąć administrator.

W niektórych przypadkach **administrator danych może jednak uznać, że przetwarzanie spełniające tylko jedno z wymienionych kryteriów będzie wymagało przeprowadzenia oceny skutków dla ochrony danych**.

Poniższe przykłady ilustrują, w jaki sposób należy korzystać z kryteriów, aby ocenić, czy dana operacja przetwarzania wymaga przeprowadzenia oceny skutków dla ochrony danych:

Przykłady przetwarzania	Ewentualne istotne kryteria	Czy istnieje prawdopodobieństwo, że wymagane będzie przeprowadzenie oceny skutków dla ochrony danych?
Szpital przetwarzający dane genetyczne i dane dotyczące zdrowia pacjenta (system informatyczny szpitala).	- Dane wrażliwe lub dane o charakterze wysoce osobistym. - Dane dotyczące osób wymagających szczególnej opieki, których dane dotyczą. - Dane przetwarzane na dużą skalę.	Tak
Zastosowanie systemu kamer monitorujących zachowanie kierowców na drogach. Administrator planuje wykorzystać inteligentny system analizy obrazu do namierzania pojedynczych samochodów i automatycznego rozpoznawania tablic rejestracyjnych.	- Systematyczne monitorowanie. - Innowacyjne wykorzystanie lub zastosowanie rozwiązań technologicznych lub organizacyjnych.	
Przedsiębiorstwo systematycznie monitoruje działania swoich pracowników, m.in. ich stanowiska pracy i aktywność w internecie *itd.*	- Systematyczne monitorowanie. - Dane dotyczące osób wymagających szczególnej opieki, których dane dotyczą.	
Gromadzenie publicznych danych z mediów społecznościowych w celu wygenerowania profilu.	- Ocena lub punktacja. - Dane przetwarzane na dużą skalę. - Dopasowanie lub łączenie zbiorów danych. - Dane wrażliwe lub dane o charakterze wysoce osobistym:	
Instytucja tworząca krajowy rating kredytowy lub bazę danych zawierającą informacje o nadużyciach finansowych.	- Ocena lub punktacja. - Automatyczne podejmowanie decyzji o skutku prawnym lub podobnie znaczącym skutku.	

Przykłady przetwarzania	Ewentualne istotne kryteria	Czy istnieje prawdopodobieństwo, że wymagane będzie przeprowadzenie oceny skutków dla ochrony danych?
	- Uniemożliwia osobom, których dane dotyczą, wykonywanie prawa lub korzystanie z usługi lub umowy. - Dane wrażliwe lub dane o charakterze wysoce osobistym:	
Przechowywanie do celów archiwizacji wrażliwych danych osobowych opatrzonych pseudonimem dotyczące osób wymagających szczególnej opieki, biorących udział w projektach badawczych lub badaniach klinicznych.	- Dane wrażliwe. - Dane dotyczące osób wymagających szczególnej opieki, których dane dotyczą. - Uniemożliwia osobom, których dane dotyczą, wykonywanie prawa lub korzystanie z usługi lub umowy.	
Przetwarzanie „danych osobowych pacjentów lub klientów [...] przez pojedynczego lekarza, innego pracownika służby zdrowia lub prawnika" (motyw 91).	- Dane wrażliwe lub dane o charakterze wysoce osobistym. - Dane dotyczące osób wymagających szczególnej opieki, których dane dotyczą.	Nie
Magazyn internetowy korzystający z listy dystrybucyjnej do wysyłania ogólnej skróconej wiadomości do swoich subskrybentów.	- Dane przetwarzane na dużą skalę.	
Strona internetowa poświęcona handlowi elektronicznemu, wyświetlająca reklamy dotyczące części do zabytkowych samochodów i korzystająca z ograniczonego profilowania w oparciu o elementy przeglądane lub kupione na tej stronie internetowej.	- Ocena lub punktacja.	

Odwrotnie, operacja przetwarzania może odpowiadać wyżej wymienionym przypadkom i nadal być uznawana przez administratora za „mogącą powodować wysokie ryzyko". W takich przypadkach administrator powinien uzasadnić i udokumentować powody, dla których nie przeprowadzono oceny skutków dla ochrony danych, oraz załączyć/zapisać poglądy inspektora ochrony danych.

Ponadto w ramach zasady rozliczalności każdy administrator danych „prowadzi rejestr czynności przetwarzania danych osobowych, za które odpowiada" obejmujący m.in. cele przetwarzania, opis kategorii danych i odbiorców danych oraz „jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1" (art. 30 ust. 1), a także musi ocenić, czy istnieje prawdopodobieństwo wystąpienia wysokiego ryzyka, nawet jeśli ostatecznie zdecyduje się nie przeprowadzać oceny skutków dla ochrony danych.

Uwaga: organy nadzorcze są zobowiązane ustanowić, podać do publicznej wiadomości i przekazać Europejskiej Radzie Ochrony Danych wykaz rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych (art. 35 ust. 4)[18]. Kryteria określone powyżej mogą pomóc organom nadzorczym w utworzeniu takiego wykazu, który w razie potrzeby można z czasem wzbogacić o bardziej szczegółowe treści. Na przykład przetwarzanie wszelkiego rodzaju danych biometrycznych lub danych dotyczących dzieci również można uznać za istotne dla opracowania wykazu zgodnego z art. 35 ust. 4.

b) Kiedy przeprowadzenie oceny skutków dla ochrony danych nie jest obowiązkowe? W przypadku, gdy nie jest prawdopodobne, aby operacja przetwarzania „mogła powodować wysokie ryzyko", gdy przeprowadzono już podobną ocenę skutków dla ochrony danych, gdy operację zatwierdzono przed majem 2018 r., lub gdy posiada podstawę prawną lub znajduje się w wykazie operacji przetwarzania, które nie podlegają ocenie skutków dla ochrony danych.

Grupa Robocza Art. 29 uważa, że ocena skutków dla ochrony danych nie jest wymagana w następujących przypadkach:

- **gdy nie jest prawdopodobne, aby operacja przetwarzania „mogła powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych"** (art. 35 ust. 1);
- **gdy charakter, zakres, kontekst i cele przetwarzania są bardzo podobne do operacji przetwarzania, w przypadku których przeprowadzono ocenę skutków dla ochrony danych**. W takich przypadkach można wykorzystać wyniki oceny skutków dla ochrony danych przeprowadzonej w odniesieniu do podobnych operacji przetwarzania (art. 35 ust. 1[19]);
- gdy operacje przetwarzania zostały sprawdzone przez organ nadzorczy przed majem 2018 r. w szczególnych warunkach, które nie uległy zmianie[20] (zob. rozdział III sekcja C);
- **jeżeli operacja przetwarzania**, zgodnie z art. 6 ust. 1 lit. c) lub e), **ma podstawę prawną** w prawie UE lub w prawie państwa członkowskiego, które reguluje daną operację przetwarzania, **oraz jeżeli oceny skutków dla ochrony danych dokonano już** w związku z przyjęciem tej podstawy prawnej (art. 35 ust. 10)[21], chyba że państwo członkowskie uznało za niezbędne dokonanie oceny skutków dla ochrony danych przed rozpoczęciem czynności przetwarzania;

[18] W tym kontekście „jeżeli wykazy […] obejmują czynności przetwarzania związane z oferowaniem towarów lub usług osobom, których dane dotyczą, lub z monitorowaniem ich zachowania w kilku państwach członkowskich lub mogące znacznie wpłynąć na swobodny przepływ danych osobowych w Unii, przed przyjęciem takich wykazów właściwy organ nadzorczy stosuje mechanizm spójności, o którym mowa w art. 63" (art. 35 ust. 6).

[19] „Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę".

[20] „Decyzje przyjęte przez Komisję oraz zezwolenia wydane przez organy nadzorcze na podstawie dyrektywy 95/46/WE pozostają w mocy do czasu ich zmiany, zastąpienia lub uchylenia" (motyw 171).

[21] Jeżeli ocena skutków dla ochrony danych przeprowadzana jest na etapie opracowywania prawodawstwa zapewniającego podstawę prawną dla przetwarzania, przegląd będzie prawdopodobnie wymagany przed rozpoczęciem operacji, ponieważ przyjęte prawodawstwo może się różnić od proponowanego w sposób, który wpływa na kwestie związane z prywatnością i ochroną danych. Ponadto w momencie przyjmowania prawodawstwa mogą nie być dostępne wystarczające szczegóły techniczne dotyczące faktycznego przetwarzania danych, nawet jeżeli przeprowadzono ocenę skutków dla ochrony danych. W takich przypadkach nadal konieczne może być dokonanie określonej oceny skutków dla ochrony danych przed rozpoczęciem rzeczywistych czynności przetwarzania.

- **jeżeli operacje przetwarzania zostały umieszczone w opcjonalnym wykazie (utworzonym przez organ nadzorczy) operacji przetwarzania** niepodlegających wymogowi dokonania oceny skutków dla ochrony danych (art. 35 ust. 5). Taki wykaz może zawierać czynności przetwarzania zgodne z warunkami określonymi przez ten organ, w szczególności poprzez wytyczne, konkretne decyzje lub zezwolenia, zasady zgodności itd. (np. we Francji: zezwolenia, zwolnienia, uproszczone zasady, pakiety zgodności itd.).W takich przypadkach i z zastrzeżeniem przeprowadzenia ponownej oceny przez właściwy organ nadzorczy przeprowadzenie oceny skutków dla ochrony danych nie jest wymagane, ale tylko wtedy, gdy przetwarzanie danych ściśle podlega zakresowi odpowiedniej procedury wymienionej w wykazie i nadal jest w pełni zgodne ze wszystkimi wymogami określonymi w RODO.

C. A co z już istniejącymi operacjami przetwarzania? W pewnych okolicznościach wymagane jest przeprowadzenie ocen skutków dla ochrony danych.

Wymóg przeprowadzenia oceny skutków dla ochrony danych dotyczy istniejących operacji przetwarzania, które mogą powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych oraz w przypadku których nastąpiła zmiana rodzaju ryzyka, z uwzględnieniem charakteru, zakresu, kontekstu i celów przetwarzania danych.

Przeprowadzenie oceny skutków dla ochrony danych nie jest wymagane w przypadku operacji przetwarzania, które zostały skontrolowane przez organ nadzorczy lub urzędnika odpowiedzialnego za ochronę danych zgodnie z art. 20 dyrektywy 95/46/WE oraz które przeprowadzono w taki sam sposób jak przed kontrolą wstępną. W istocie „decyzje przyjęte przez Komisję oraz zezwolenia wydane przez organy nadzorcze na podstawie dyrektywy 95/46/WE pozostają w mocy do czasu ich zmiany, zastąpienia lub uchylenia" (motyw 171).

Z drugiej strony oznacza to, że oceną skutków dla ochrony danych należy objąć wszelkie operacje przetwarzania danych, w odniesieniu do których od czasu przeprowadzenia kontroli wstępnej przez organ nadzorczy lub urzędnika odpowiedzialnego za ochronę danych zmieniły się warunki wdrażania (zakres, cel, zgromadzone dane osobowe, tożsamość administratorów danych lub odbiorców, okres zatrzymywania danych, środki techniczne i organizacyjne itd.) i które mogą powodować wysokie ryzyko.

Ponadto przeprowadzenie oceny skutków dla ochrony danych może być wymagane po zmianie rodzaju ryzyka związanego z operacją przetwarzania[22], np. z powodu wykorzystania nowej technologii lub dlatego, że dane osobowe wykorzystywane są w innym celu. Operacje przetwarzania danych mogą szybko ewoluować i mogą pojawić się nowe zagrożenia. Należy zatem zauważyć, że przegląd oceny skutków dla ochrony danych jest użyteczny nie tylko dla ciągłego doskonalenia, ale ma również kluczowe znaczenie dla utrzymania w przyszłości poziomu ochrony danych w zmieniającym się środowisku. Przeprowadzenie oceny skutków dla ochrony danych może być również konieczne ze względu na zmianę kontekstu organizacyjnego lub społecznego czynności przetwarzania, np. ponieważ skutki niektórych automatycznie podjętych decyzji stały się bardziej znaczące lub ponieważ nowe kategorie osób, których dane dotyczą, są narażone na dyskryminację. Każdy z tych przykładów może być elementem prowadzącym do zmiany ryzyka związanego z daną czynnością przetwarzania.

[22] Pod względem kontekstu, zgromadzonych danych, celów, funkcji, przetwarzanych danych osobowych, odbiorców, kombinacji danych (aktywa pomocnicze, źródła ryzyka, potencjalne skutki, zagrożenia itd.), środków bezpieczeństwa i międzynarodowego przekazywania danych.

Z drugiej strony niektóre zmiany mogłyby również zmniejszyć ryzyko. Na przykład operacja przetwarzania może ewoluować w taki sposób, że decyzje nie będą już podejmowane automatycznie, lub działania monitorujące przestaną być realizowane systematycznie. W tym przypadku przegląd przeprowadzonej analizy ryzyka może wykazać, że nie ma już potrzeby przeprowadzenia oceny skutków dla ochrony danych.

Dobrą praktyką powinno być **stałe przeprowadzanie przeglądu oceny skutków dla ochrony danych i regularne przeprowadzanie ponownej oceny**. W związku z powyższym, nawet jeżeli w dniu 25 maja 2018 r. nie wymaga się przeprowadzenia oceny skutków dla ochrony danych, administrator będzie musiał w odpowiednim momencie przeprowadzić taką ocenę w ramach swoich ogólnych obowiązków w zakresie rozliczalności.

D. Jak przeprowadzić ocenę skutków dla ochrony danych?

a) W jakim momencie należy przeprowadzić ocenę skutków dla ochrony danych? Przed rozpoczęciem przetwarzania.

Ocenę skutków dla ochrony danych należy przeprowadzić „przed rozpoczęciem przetwarzania" (art. 35 ust. 1 i 10, motywy 90 i 93)[23]. Jest to zgodne z zasadami dotyczącymi uwzględniania ochrony danych w fazie projektowania oraz domyślnej ochrony danych (art. 25 i motyw 78). Ocenę skutków dla ochrony danych należy postrzegać jako narzędzie wspomagające proces podejmowania decyzji w sprawie przetwarzania danych.

Ocena skutków dla ochrony danych powinna rozpocząć się jak najwcześniej w fazie projektowania operacji przetwarzania, nawet jeżeli niektóre operacje przetwarzania nadal są nieznane. Aktualizacja oceny skutków dla ochrony danych przez cały cykl trwania projektu zapewni uwzględnienie ochrony danych i prywatności oraz zachęci do tworzenia rozwiązań promujących zgodność. W miarę postępu procesu rozwoju konieczne może być również powtórzenie poszczególnych etapów oceny, ponieważ wybór niektórych środków technicznych lub organizacyjnych może wpłynąć na prawdopodobieństwo wystąpienia zagrożenia wynikającego z przetwarzania lub jego wagę.

Fakt, że aktualizacja oceny skutków dla ochrony danych może okazać się konieczna już po rozpoczęciu procesu przetwarzania, nie uzasadnia odroczenia lub nieprzeprowadzenia oceny skutków dla ochrony danych. Ocena skutków dla ochrony danych jest procesem ciągłym, szczególnie gdy operacja przetwarzania przebiega dynamicznie i podlega ciągłym zmianom. **Prowadzenie oceny skutków dla ochrony danych jest procesem ciągłym, a nie jednorazowym.**

b) Kto jest zobowiązany do przeprowadzenia oceny skutków dla ochrony danych? Administrator, wspólnie z DPO i podmiotem przetwarzającym.

Administrator jest odpowiedzialny za zapewnienie przeprowadzenia oceny skutków dla ochrony danych (art. 35 ust. 2). Ocenę skutków dla ochrony danych może przeprowadzić inny podmiot, zarówno z danej jednostki, jak i spoza niej, jednak ostateczna odpowiedzialność za wykonanie zadania spoczywa na administratorze.

[23] Z wyjątkiem przypadków, gdy jest to już istniejąca operacja przetwarzania, która została poddana kontroli wstępnej przez organ nadzorczy. W takim przypadku ocenę skutków dla ochrony danych należy przeprowadzić przed wprowadzeniem znaczących zmian.

Administrator musi również konsultować się z inspektorem ochrony danych (DPO), o ile został on wyznaczony (art. 35 ust. 2), a wyniki konsultacji i podjęte decyzje powinien udokumentować w ramach oceny skutków dla ochrony danych. DPO powinien również monitorować wykonanie oceny skutków dla ochrony danych (art. 39 ust. 1 lit. c)). Dalsze wskazówki można znaleźć w wytycznych Grupy Roboczej Art. 29 dotyczących inspektora ochrony danych 16/EN WP 243.

Jeżeli proces przetwarzania jest całkowicie lub częściowo realizowany przez podmiot przetwarzający dane, **podmiot przetwarzający powinien pomóc administratorowi danych w przeprowadzeniu oceny skutków dla ochrony danych** i dostarczyć wszelkie niezbędne informacje (zgodnie z art. 28 ust. 3 lit. f)).

„W stosownych przypadkach" administrator musi „zasięgnąć opinii osób, których dane dotyczą, lub ich przedstawicieli" (art. 35 ust. 9). Grupa Robocza Art. 29 uważa, że:

- opinie te można zebrać za pomocą różnych środków, w zależności od kontekstu (np. badanie ogólne dotyczące celu i środków operacji przetwarzania, pytanie do przedstawicieli pracowników lub zwykła ankieta wysłana do przyszłych klientów administratora danych), zapewniając, aby administrator miał podstawę prawną do przetwarzania wszelkich danych osobowych wykorzystywanych podczas zbierania takich opinii. Należy jednak zauważyć, że zgoda na przetwarzanie nie jest oczywiście sposobem na uzyskanie opinii osób, których dane dotyczą;
- jeżeli ostateczna decyzja administratora danych różni się od opinii osób, których dane dotyczą, należy udokumentować powody podjęcia, bądź niepodjęcia decyzji;
- administrator powinien również przedstawić uzasadnienie niezasięgnięcia opinii osób, których dane dotyczą, jeżeli uzna to za niewłaściwe, np. w przypadku gdy stanowiłoby ono zagrożenie dla poufności biznesplanów przedsiębiorstw lub byłoby nieproporcjonalne lub niewykonalne.

Ponadto dobrą praktyką jest zdefiniowanie i udokumentowanie innych konkretnych ról i obowiązków, w zależności od polityki wewnętrznej, procesów i zasad np.:

- w przypadku gdy poszczególne jednostki gospodarcze mogą zaproponować przeprowadzenie oceny skutków dla ochrony danych, powinny one dostarczyć dane wejściowe dotyczące tej oceny i powinny uczestniczyć w procesie zatwierdzania oceny;
- w stosownych przypadkach zaleca się zasięgnięcie opinii niezależnych ekspertów reprezentujących różne zawody[24] (prawników, informatyków, ekspertów z zakresu bezpieczeństwa, socjologów, etyków *itp.*);
- role i obowiązki podmiotów przetwarzających muszą zostać określone w umowie; zaś ocenę skutków dla ochrony danych należy przeprowadzić z pomocą podmiotu przetwarzającego, uwzględniając charakter przetwarzania oraz dostępne mu informacje (art. 28 ust. 3 lit. f));
- główny urzędnik ds. bezpieczeństwa informacji, o ile został powołany, oraz DPO mogą zasugerować administratorowi przeprowadzenie oceny skutków dla ochrony danych w odniesieniu do konkretnej operacji przetwarzania oraz powinni pomóc zainteresowanym stronom w opracowaniu metodyki, w ocenie jakości oceny ryzyka, w stwierdzeniu, czy dopuszczalne jest ryzyko szczątkowe, oraz w rozwijaniu wiedzy odpowiedniej dla administratora danych;

[24] *Zalecenia dotyczące ram oceny skutków w zakresie prywatności dla Unii Europejskiej, rezultat D3*: http://www.piafproject.eu/ref/PIAF_D3_final.pdf

- główny urzędnik ds. bezpieczeństwa informacji, o ile został powołany, lub pracownik działu IT, powinien zapewnić pomoc administratorowi oraz może zaproponować przeprowadzenie oceny skutków dla ochrony danych w odniesieniu do konkretnej operacji przetwarzania, w zależności od potrzeb operacyjnych i potrzeb związanych z bezpieczeństwem.

c) Zgodnie z jaką metodyką przeprowadza się ocenę skutków dla ochrony danych? Różna metodyka, wspólne kryteria.

W RODO określono minimalne cechy, jakie powinna posiadać ocena skutków dla ochrony danych (art. 35 ust. 7 oraz motywy 84 i 90), a mianowicie:

- „opis planowanych operacji przetwarzania i celów przetwarzania";
- „ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne";
- „ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą";
- „środki planowane w celu":
  - „zaradzenia ryzyku;"
  - „wykazania przestrzegania niniejszego rozporządzenia".

Na poniższym wykresie przedstawiono generyczny, iteracyjny proces przeprowadzania oceny skutków dla ochrony danych[25]:



Podczas oceny skutków operacji przetwarzania danych należy uwzględnić zgodność (art. 35 ust. 8) z kodeksem postępowania (art. 40). Może to być przydatne w celu wykazania, że wybrano lub wprowadzono odpowiednie środki, pod warunkiem że kodeks postępowania jest odpowiedni dla operacji przetwarzania. Uwzględnić należy również certyfikacje, znaki jakości oraz oznaczenia mające świadczyć o zgodności z RODO operacji przetwarzania prowadzonych przez administratorów i podmioty przetwarzające (art. 42), a także wiążące reguły korporacyjne.

Wszystkie właściwe wymogi określone w RODO zapewniają szerokie, generyczne ramy służące do opracowania i przeprowadzania oceny skutków dla ochrony danych. Praktyczne wdrożenie oceny skutków dla ochrony danych będzie uzależnione od wymogów określonych w RODO, które można

[25] Należy podkreślić, że przedstawiony tutaj proces ma charakter iteracyjny: w praktyce prawdopodobne jest, że przed zakończeniem oceny skutków dla ochrony danych każdy z etapów będzie wielokrotnie powtarzany.

uzupełnić bardziej szczegółowymi praktycznymi wytycznymi. Wdrożenie oceny skutków dla ochrony danych jest zatem skalowalne. Oznacza to, że nawet administrator danych działający na małą skalę może opracować i wdrożyć ocenę skutków dla ochrony danych, która jest odpowiednia do danych operacji przetwarzania.

W motywie 90 RODO przedstawiono szereg elementów składowych oceny skutków dla ochrony danych, które pokrywają się z dobrze określonymi składowymi zarządzania ryzykiem (np. ISO 31000[26]). Z perspektywy zarządzania ryzykiem ocena skutków dla ochrony danych ma na celu „zarządzanie czynnikami ryzyka" naruszenia praw i wolności osób fizycznych, z wykorzystaniem poniższych procesów, poprzez:

- określanie kontekstu: „uwzględnienie charakteru, zakresu, kontekstu i celów przetwarzania oraz źródeł ryzyka";
- dokonywanie oceny ryzyka: „ocena konkretnego prawdopodobieństwa i powagi tego wysokiego ryzyka";
- traktowanie ryzyka: „minimalizowanie tego ryzyka" i „zapewnienie ochrony danych osobowych", a także „wykazanie przestrzegania niniejszego rozporządzenia".

Uwaga: ocena skutków dla ochrony danych, o której mowa w RODO, stanowi narzędzie służące do zarządzania ryzykiem naruszenia praw osób, których dane dotyczą, a zatem przy jej przeprowadzaniu przyjmuje się ich perspektywę, podobnie jak w przypadku określonych dziedzin (np. bezpieczeństwo społeczne). Z kolei zarządzanie ryzykiem w pozostałych dziedzinach (np. bezpieczeństwa informacji) skupia się na organizacji.

Za pośrednictwem RODO zapewniono administratorom danych elastyczność przy określaniu dokładnej struktury i formy oceny skutków dla ochrony danych w celu umożliwienia jej dopasowania do istniejących praktyk roboczych. W UE i na całym świecie istnieje szereg różnych określonych procesów, w przypadku których uwzględniono elementy składowe opisane w motywie 90. Niezależnie od formy ocena skutków dla ochrony danych musi jednak stanowić rzeczywistą ocenę ryzyka, pozwalając administratorom podjąć działania na rzecz wyeliminowania ryzyka.

Można zastosować różne metodyki (przykłady metodyki ochrony danych i oceny skutków w zakresie prywatności znajdują się załączniku 1), aby wspomóc wdrażanie podstawowych wymogów określonych w RODO. Określono wspólne kryteria mające umożliwić stosowanie tych różnych podejść, a jednocześnie pozwolić administratorom na zachowanie zgodności z RODO (zob. załącznik 2). Za pomocą tych kryteriów uściślono podstawowe wymogi zawarte w rozporządzeniu, lecz przewidziano wystarczający zakres swobody, aby możliwe były różne formy wdrażania. Kryteria te można wykorzystać do wykazania, że konkretna metodyka oceny skutków dla ochrony danych spełnia standardy przewidziane w RODO. **Decyzję o wyborze metodyki podejmuje administrator danych, lecz metodyka ta powinna być zgodna z kryteriami określonymi w załączniku 2.**

Grupa Robocza Art. 29 zachęca do opracowywania ram oceny skutków dla ochrony danych dla poszczególnych sektorów. Wynika to z faktu, że jej członkowie mogą oprzeć się na specyficznej dla danego sektora wiedzy, co oznacza, że ocenę skutków dla ochrony danych można ukierunkować na konkretny rodzaj operacji przetwarzania (np. konkretne rodzaje danych, majątku wspólnego,

[26] Procesy zarządzania ryzykiem: komunikacja i konsultacja, określanie kontekstu, ocena ryzyka, traktowanie ryzyka, monitorowanie i przegląd (zob. pojęcia i definicje oraz spis treści w przeglądzie ISO 31000: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en).

możliwych skutków, zagrożeń, działań). Oznacza to, że ocena skutków dla ochrony danych może zaradzić problemom, które powstają w konkretnym sektorze gospodarki, przy stosowaniu konkretnych technologii lub przy przeprowadzaniu operacji przetwarzania określonego rodzaju.

Ponadto w razie potrzeby „przynajmniej gdy zmienia się ryzyko wynikające z operacji przetwarzania, administrator dokonuje przeglądu, by stwierdzić, czy przetwarzanie odbywa się zgodnie z oceną skutków dla ochrony danych" (art. 35 ust. 11[27]).

d) Czy publikacja oceny skutków dla ochrony danych jest obowiązkowa? Nie, lecz publikacja podsumowania może przyczynić się do zwiększenia zaufania, a pełną treść oceny skutków dla ochrony danych należy przekazać organom nadzorczym, jeżeli miały miejsce uprzednie konsultacje lub jeżeli zwrócił się o to organ ochrony danych.

RODO nie zawiera prawnego wymogu publikacji oceny skutków dla ochrony danych; decyzja o publikacji należy do administratora. Administratorzy powinni jednakże rozważyć publikację choćby części przeprowadzonych przez nich ocen skutków dla ochrony danych, takich jak podsumowanie lub wnioski.

Proces taki miałby na celu przyczynienie się do zwiększenia zaufania, którym obdarza się administratora dokonującego operacji przetwarzania, i do wykazania rozliczalności i przejrzystości. Szczególnie dobrą praktyką jest publikowanie oceny skutków dla ochrony danych, jeżeli operacja przetwarzania ma wpływ na społeczeństwo. Może to dotyczyć szczególnie przypadków, w których ocenę skutków dla ochrony danych przeprowadza organ publiczny.

Opublikowana wersja oceny skutków dla ochrony danych nie musi zawierać całej oceny, szczególnie w przypadku, gdy ocena skutków dla ochrony danych mogłaby zawierać szczegółowe informacje na temat rodzajów ryzyka dla bezpieczeństwa odnoszących się do administratora danych lub wyjawiać tajemnice przedsiębiorstwa lub szczególnie chronione informacje handlowe. W takich okolicznościach wersja opublikowana może składać się zaledwie z podsumowania głównych ustaleń dokonanych w toku oceny skutków dla ochrony danych lub wyłącznie z oświadczenia, że przeprowadzono ocenę skutków dla ochrony danych.

Ponadto jeżeli w toku oceny skutków dla ochrony danych ujawniono istnienie wysokiego ryzyka szczątkowego, administrator danych będzie zobowiązany zwrócić się do organu nadzorczego o uprzednie konsultacje dotyczące przetwarzania (art. 36 ust. 1). W ramach tych konsultacji należy przedstawić pełną ocenę skutków dla ochrony danych (art. 36 ust. 3 lit. e)). Organ nadzorczy może udzielić zalecenia[28] i nie naruszy tajemnicy przedsiębiorstwa ani nie ujawni luk w zabezpieczeniach, z zastrzeżeniem mających zastosowanie w każdym państwie członkowskim zasad publicznego dostępu do dokumentów urzędowych.

E. Kiedy należy skonsultować się z organem nadzorczym? Jeżeli ryzyko szczątkowe jest wysokie.

Jak wyjaśniono powyżej:

[27] W art. 35 ust. 10 wyraźnie wyłączono zastosowanie jedynie art. 35 ust. 1–7.

[28] W myśl art. 36 ust. 2 udzielenie administratorowi pisemnego zalecenia jest niezbędne wyłącznie w przypadku, gdy organ nadzorczy jest zdania, że zamierzone przetwarzanie nie jest zgodne z rozporządzeniem.

- przeprowadzenie oceny skutków dla ochrony danych jest wymagane w przypadku, gdy operacja przetwarzania „może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych" (art. 35 ust. 1, zob. rozdział III sekcja B lit. b)). Przykładowo przetwarzanie danych dotyczących zdrowia na dużą skalę uważa się za mogące powodować wysokie ryzyko i wymaga ono przeprowadzenia oceny skutków dla ochrony danych;
- w takim przypadku obowiązkiem administratora danych jest dokonanie oceny ryzyka naruszenia praw i wolności osób, których dane dotyczą, oraz zidentyfikowanie środków[29] planowanych w celu zmniejszenia tego ryzyka do dopuszczalnego poziomu i wykazania przestrzegania RODO (art. 35 ust. 7, zob. rozdział III sekcja C lit. c)). Przykładem, jeżeli chodzi o przechowywanie danych osobowych na laptopach, może być zastosowanie odpowiednich technicznych i organizacyjnych środków bezpieczeństwa (skuteczne szyfrowanie całego dysku, solidne zarządzanie kluczami, odpowiednia kontrola dostępu, zabezpieczone kopie zapasowe, itd.) uzupełniających środki stosowane w ramach istniejącej polityki (zawiadomienie, zgoda, prawo dostępu, prawo wniesienia sprzeciwu, itd.).

Jeżeli w przywołanym powyżej przykładzie dotyczącym laptopa administrator danych uznał ryzyko za dostatecznie ograniczone i można je za takie uznać zgodnie z brzmieniem art. 36 ust. 1 i motywów 84 i 94, przetworzenia można dokonać bez konsultacji z organem nadzorczym. Administrator danych musi skonsultować się z organem nadzorczym w sytuacji, gdy nie może dostatecznie ograniczyć zidentyfikowanego ryzyka (np. utrzymuje się wysokie ryzyko szczątkowe).

Przykład niedopuszczalnego wysokiego ryzyka szczątkowego obejmuje przypadki, w których osoby, których dane dotyczą, mogą ponieść znaczne lub nawet nieodwracalne konsekwencje, z którymi nie będą mogły sobie poradzić (np.: bezprawne uzyskanie dostępu do danych prowadzące do zagrożenia życia osób, których dane dotyczą, zwolnienie, zagrożenie o charakterze finansowym) lub w których wydaje się oczywiste, że wystąpi ryzyko (np.: ograniczenie liczby osób mających dostęp do danych nie jest możliwy ze względu na sposób ich udostępniania, wykorzystywania lub rozprowadzania lub gdy luka w zabezpieczeniach, o której istnieniu wiadomo, nie zostanie usunięta).

Zawsze gdy administrator danych nie może znaleźć środków wystarczających do zmniejszenia ryzyka do dopuszczalnego poziomu (np. ryzyko szczątkowe wciąż jest wysokie), wymagane są konsultacje z organem nadzorczym[30].

Ponadto administrator będzie zobowiązany skonsultować się z organem nadzorczym zawsze, gdy prawo państwa członkowskiego wymaga, by administratorzy konsultowali się z organem nadzorczym lub uzyskiwali jego uprzednią zgodę w odniesieniu do przetwarzania danych osobowych przez administratora do celów wykonania zadania realizowanego przez niego w interesie publicznym, w tym przetwarzania w związku z ochroną socjalną i zdrowiem publicznym (art. 36 ust. 5).

Należy jednak zaznaczyć, że niezależnie od tego, czy wymagane są konsultacje z organem nadzorczym na podstawie poziomu ryzyka szczątkowego, obowiązki polegające na przechowywaniu

[29] W tym uwzględnienie istniejących wytycznych od Europejskiej Rady Ochrony Danych i organów nadzorczych oraz uwzględnienie stanu techniki i kosztów wdrażania, jak określono w art. 35 ust. 1.

[30] Uwaga: „pseudonimizacja oraz szyfrowanie danych osobowych" (a także minimalizacja danych, mechanizmu nadzoru itd.) niekoniecznie stanowią odpowiednie środki. Stanowią one jedynie przykłady. W zależności od kontekstu i ryzyka odpowiednie są różne środki, właściwe dla operacji przetwarzania.

dokumentacji związanej z oceną skutków dla ochrony danych i dokonywaniu aktualizacji oceny skutków dla ochrony danych w stosownym terminie, pozostają aktualne.

IV. Wnioski i zalecenia

Oceny skutków dla ochrony danych stanowią przydatne narzędzie wykorzystywane przez administratorów danych do wdrażania systemów przetwarzania danych, które są zgodne z RODO, a przeprowadzenie tych ocen może okazać się obowiązkowe w przypadku niektórych rodzajów operacji przetwarzania. Oceny skutków dla ochrony danych są skalowalne i mogą przybierać różne formy, lecz w RODO określono podstawowe wymogi skutecznej oceny skutków dla ochrony danych. Administratorzy danych powinni postrzegać dokonywanie oceny skutków dla ochrony danych jako przydatne i pozytywne działanie, które przyczynia się do zachowania zgodności z prawem.

W art. 24 ust. 1 określono podstawowy obowiązek administratora w zakresie zachowania zgodności z RODO: „uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane".

Dokonywanie oceny skutków dla ochrony danych ma zasadnicze znaczenie dla zachowania zgodności z rozporządzeniem, jeżeli planuje się lub odbywa się przetwarzanie danych, z którym wiąże się wysokie ryzyko. Oznacza to, że administratorzy danych powinni stosować kryteria określone w niniejszym dokumencie w celu ustalenia, czy należy dokonać oceny skutków dla ochrony danych. W ramach wewnętrznej polityki stosowanej przez administratorów danych można rozszerzyć ten wykaz poza wymogi prawne zawarte w RODO. Powinno to skutkować większym zaufaniem osób, których dotyczą dane, i pozostałych administratorów danych i uzyskaniem przez nich pewności.

W przypadku gdy planuje się przetwarzanie mogące powodować wysokie ryzyko, administrator danych musi:

- wybrać metodykę dokonywania oceny skutków dla ochrony danych (przykłady podano w załączniku 1), która spełnia kryteria określone w załączniku 2, lub określić i wdrożyć systematyczny proces dokonywania oceny skutków dla ochrony danych, który:
  - jest zgodny z kryteriami zawartymi w załączniku 2;
  - jest zintegrowany z istniejącym procesami projektowania, opracowywania, zmian, ryzyka i przeglądu operacyjnego zgodnie z procesami wewnętrznymi, kontekstem i kulturą;
  - angażuje strony, których sprawa dotyczy, i w ramach, którego jasno określono ich obowiązki (administratora, DPO, osób, których dane dotyczą, lub ich przedstawicieli, przedsiębiorstw, służb technicznych, podmiotów przetwarzających, inspektora ds. bezpieczeństwa informacji, itd.);
- przedłożyć właściwym organom nadzorczym sprawozdanie z oceny skutków dla ochrony danych, gdy jest to wymagane;
- konsultować się z organem nadzorczym, jeżeli określenie środków wystarczających do zminimalizowania wysokiego ryzyka zakończyło się niepowodzeniem;
- okresowo dokonywać przeglądu oceny skutków dla ochrony danych i przetwarzania, którego oceny dokonano w jej ramach, przynajmniej gdy doszło do zmiany ryzyka wynikającego z przetwarzania operacji;
- dokumentować podjęte decyzje.

Załącznik 1 – Przykłady istniejących unijnych ram dokonywania oceny skutków dla ochrony danych

W RODO nie określono, który proces dokonywania oceny skutków dla ochrony danych należy stosować, ale za to umożliwiono administratorom danych wprowadzanie ram, które uzupełniają dotychczas przez nich stosowane praktyki robocze, o ile uwzględniają one elementy składowe opisane w art. 35 ust. 7. Takie ramy mogą być dopasowane do indywidualnych potrzeb administratora danych lub wspólne dla całej określonej branży. Wcześniej opublikowane ramy, opracowane przez unijne organy ochrony danych oraz stosowane w UE ramy dla poszczególnych sektorów obejmują (m.in.):

przykłady stosowanych w UE ogólnych ram:

- DE: standardowy model ochrony danych, V.1.0 – wersja próbna, 2016 r.[31].
  https://www.datenschutzzentrum.de/uploads/SDM-Methodology_V1_EN1.pdf
- ES: „Guía para una Evaluación de Impacto en la Protección de Datos Personales (EIPD)", Agencia española de protección de datos (AGPD), 2014 r.
  https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf
- FR: ocena skutków w zakresie prywatności, Commission nationale de l'informatique et des libertés (CNIL), 2015 r.
  https://www.cnil.fr/fr/node/15798
- UK: kodeks praktyk w zakresie dokonywania oceny skutków w zakresie prywatności (Conducting privacy impact assessments code of practice), Biuro Komisarza ds. Informacji, 2014 r.
  https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

przykłady stosowanych w UE ram dla poszczególnych sektorów:

- ramy oceny skutków dla ochrony danych i prywatności w zastosowaniach RFID[32].
  http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_annex_en.pdf
- szablon oceny skutków dla ochrony danych na potrzeby inteligentnych sieci i inteligentnych systemów pomiarowych[33]
  http://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf

[31] Zatwierdzony jednomyślnie i przez aklamację (przy wstrzymującej się Bawarii) na 92. konferencji niezależnych organów ochrony danych z federacji i krajów związkowych, która odbyła się w Kühlungsborn w dniach 9–10 listopada 2016 r.

[32] Zob. również:

- zalecenie Komisji z dnia 12 maja 2009 r. w sprawie wdrażania zasad ochrony prywatności i ochrony danych w zastosowaniach wspieranych identyfikacją radiową.
  https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-12-may-2009-implementation-privacy-and-data-protection-principles
- opinia 9/2011 na temat zmienionej propozycji sektora w sprawie ram oceny skutków w zakresie ochrony danych i prywatności w zastosowaniach RFID.
  http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_pl.pdf

[33] Zob. również opinia 07/2013 w sprawie szablonu oceny skutków dla ochrony danych na potrzeby inteligentnych sieci i inteligentnych systemów pomiarowych opracowanego przez grupę ekspertów nr 2 w ramach grupy zadaniowej ds. inteligentnych sieci Komisji. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp209_en.pdf

W ramach normy międzynarodowej zapewnione zostaną również wytyczne dotyczące metodyk stosowanych do dokonywania oceny skutków dla ochrony danych (ISO/IEC 29134[34]).

[34] ISO/IEC 29134 (projekt), IT – Techniki bezpieczeństwa – ocena skutków w zakresie prywatności – Wytyczne, Międzynarodowa Organizacja Normalizacyjna (ISO).

Załącznik 2 – Kryteria dopuszczalnej oceny skutków dla ochrony danych

Grupa Robocza Art. 29 proponuje następujące kryteria, z których administratorzy danych mogą korzystać, aby ocenić, czy ocena skutków dla ochrony danych lub metodyka służąca do dokonania oceny skutków dla ochrony danych są wystarczająco kompleksowe do zachowania zgodności z RODO:

- ☐ zapewniono systematyczny opis operacji przetwarzania (art. 35 ust. 7 lit. a)):
  - ☐ uwzględniono charakter, zakres, kontekst i cele przetwarzania (motyw 90);
  - ☐ w rejestrze zamieszczono dane osobowe, informacje o odbiorcach i okresie przechowywania danych osobowych;
  - ☐ przedstawiono funkcjonalny opis operacji przetwarzania;
  - ☐ zidentyfikowano zasoby, z którymi styczność mają dane osobowe (sprzęt komputerowy, oprogramowanie, sieci, osoby, opracowania lub kanały transmisji opracowań);
  - ☐ uwzględniono przestrzeganie zatwierdzonych kodeksów postępowania (art. 35 ust. 8);
- ☐ oceniono niezbędność oraz proporcjonalność (art. 35 ust. 7 lit. b)):
  - ☐ wskazano środki, których podjęcie jest planowane w celu zapewnienia przestrzegania rozporządzenia (art. 35 ust. 7 lit. d) i motyw 90), uwzględniając:
    - ☐ środki przyczyniające się do proporcjonalności i niezbędności przetwarzania, z uwzględnieniem następujących aspektów:
      - ☐ konkretne, wyraźne i prawnie uzasadnione cele (art. 5 ust. 1 lit. b));
      - ☐ zgodność przetwarzania z prawem (art. 6);
      - ☐ dane adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane (art. 5 ust. 1 lit. c));
      - ☐ ograniczony czas przechowywania (art. 5 ust. 1 lit. e));
    - ☐ środki przyczyniające się do zachowania praw osób, których dane dotyczą:
      - ☐ poinformowanie osoby, której dane dotyczą (art. 12, 13 i 14);
      - ☐ prawo dostępu i prawo do przenoszenia danych (art. 15 i 20);
      - ☐ prawo do sprostowania i do usunięcia danych (art. 16, 17 i 19);
      - ☐ prawo do sprzeciwu i prawo do ograniczenia przetwarzania (art. 18, 19 i 21);
      - ☐ relacje z podmiotem przetwarzającym (art. 28);
      - ☐ zabezpieczenia przy międzynarodowym przekazywaniu danych (rozdział V);
      - ☐ uprzednie konsultacje (art. 36);
- ☐ przeprowadzono działania w zakresie zarządzania ryzykiem naruszenia praw i wolności osób, których dane dotyczą (art. 35 ust. 7 lit. c)):
  - ☐ uwzględniono źródło, charakter, specyfikę i powagę ryzyka (por. motyw 84), czy konkretniej, w przypadku każdego rodzaju ryzyka (bezprawnego dostępu, niepożądanej zmiany i zniknięcia danych), z punktu widzenia osób, których dane dotyczą:
    - ☐ uwzględniono źródła ryzyka (motyw 90);
    - ☐ zidentyfikowano możliwe skutki dla praw i wolności osób, których dane dotyczą, w przypadku zdarzeń takich jak bezprawny dostęp, niepożądane zmiany i zniknięcie danych;
    - ☐ zidentyfikowano zagrożenia, które mogłyby doprowadzić do bezprawnego dostępu, niepożądanych zmian i zniknięcia danych;
    - ☐ oszacowano prawdopodobieństwo i powagę (motyw 90);
  - ☐ określono środki, których podjęcie jest planowane w celu zaradzenia ryzyku (art. 35 ust. 7 lit. d) i motyw 90);
- ☐ zaangażowano zainteresowane strony:
  - ☐ skonsultowano się z inspektorem ochrony danych w celu uzyskania zalecenia (art. 35 ust. 2);

- ☐ w stosownych przypadkach zasięgnięto opinii osób, których dane dotyczą, lub ich przedstawicieli (art. 35 ust. 9).

GRUPA ROBOCZA ART. 29

16/EN
WP 242 rev.01

Wytyczne dotyczące prawa do przenoszenia danych

Przyjęte w dniu 13 grudnia 2016 r.
Ostatnio zmienione i przyjęte w dniu 5 kwietnia 2017 r.

Grupa Robocza została powołana na mocy art. 29 dyrektywy 95/46/WE. Jest ona niezależnym europejskim organem doradczym w zakresie ochrony danych i prywatności. Zadania Grupy zostały określone w przepisach art. 30 dyrektywy 95/46/WE i art. 15 dyrektywy 2002/58/WE.

Obsługę sekretariatu zapewnia Dyrekcja C (prawa podstawowe i praworządność) Dyrekcji Generalnej ds. Sprawiedliwości i Konsumentów Komisji Europejskiej, B-1049 Bruksela, Belgia, biuro nr MO59 05/35.

Strona internetowa: http://ec.europa.eu/justice/data-protection/index_en.htm

SPIS TREŚCI

Streszczenie **3**
I. Wprowadzenie **4**
II. Jakie są główne elementy przenoszenia danych? **5**
III. W jakich sytuacjach ma zastosowanie przenoszenie danych? **9**
IV. W jaki sposób do przenoszenia danych stosuje się przepisy ogólne regulujące wykonywanie praw przysługujących osobie, której dane dotyczą.? **15**
V. W jaki sposób należy przekazywać dane podlegające przenoszeniu? **18**

Streszczenie

W art. 20 ogólnego rozporządzenia o ochronie danych (RODO) ustanowiono nowe prawo do przenoszenia danych, które jest ściśle związane z prawem dostępu, ale pod wieloma względami się od niego różni. Prawo to umożliwia osobom, których dane dotyczą, otrzymanie w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego danych osobowych, które dostarczyły one administratorowi, oraz przesłanie tych danych osobowych innemu administratorowi. Celem tego nowego prawa jest wzmocnienie pozycji osoby, której dane dotyczą, i przyznanie jej większej kontroli nad danymi osobowymi jej dotyczącymi.

Prawo do przenoszenia danych umożliwia przesłanie danych osobowych przez jednego administratora bezpośrednio innemu administratorowi, w związku z czym jest ono również istotnym narzędziem, które wesprze swobodny przepływ danych osobowych w UE i będzie sprzyjać konkurencji między administratorami. Ułatwi ono zmianę dostawców usług i tym samym będzie sprzyjać rozwojowi nowych usług w kontekście strategii jednolitego rynku cyfrowego.

W opinii tej przedstawiono wytyczne dotyczące sposobu interpretacji i wdrożenia prawa do przenoszenia danych określonego w RODO. Ma ona na celu omówienie prawa do przenoszenia danych i zakresu jego stosowania. W opinii wyjaśniono warunki, pod jakimi to nowe prawo ma zastosowanie, z uwzględnieniem podstawy prawnej przetwarzania danych (zgody osoby, której dane dotyczą, albo konieczności wykonania umowy) oraz faktu, że prawo to ogranicza się do danych osobowych dostarczonych przez osobę, której dane dotyczą. Przedstawiono w niej również konkretne przykłady i kryteria, aby wyjaśnić okoliczności, w których prawo to ma zastosowanie. W tym względzie Grupa Robocza Art. 29 uważa, że prawo do przenoszenia danych obejmuje dane świadomie i czynnie dostarczone przez osobę, której dane dotyczą, oraz dane osobowe wygenerowane w wyniku działania tej osoby. Tego nowego prawa nie można naruszać i nie można go ograniczyć do danych osobowych przekazanych bezpośrednio przez osobę, której dane dotyczą, np. w formularzu online.

W ramach dobrej praktyki administratorzy danych powinni rozpocząć prace nad środkami, które będą pomocne przy udzielaniu odpowiedzi na żądania o przeniesienie danych, takimi jak narzędzia do pobierania i interfejsy programowania aplikacyjnego. Powinni oni zagwarantować, że dane osobowe przekazuje się w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego, przy czym należy ich zachęcać, aby zapewnili interoperacyjność formatu, w którym dane przekazano w odpowiedzi na żądanie o przeniesienie danych.

Opinia pomaga również administratorom danych dokładnie zrozumieć ich poszczególne obowiązki, a także zawiera zalecenia odnośnie do najlepszych praktyk i narzędzi wspierających zgodność z prawem do przenoszenia danych. Ponadto w opinii zaleca się zainteresowanym stronom w branży i stowarzyszeniom branżowym współpracę nad opracowaniem wspólnego zbioru standardów i formatów interoperacyjnych celem spełnienia wymogów dotyczących prawa do przenoszenia danych.

I. Wprowadzenie

W art. 20 ogólnego rozporządzenia o ochronie danych (RODO) wprowadzono nowe prawo do przenoszenia danych. Prawo to umożliwia osobom, których dane dotyczą, otrzymanie w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego danych osobowych dostarczonych przez te osoby administratorowi danych oraz przesłanie, bez przeszkód, tych danych osobowych innemu administratorowi danych. To prawo, które stosuje się przy spełnieniu określonych warunków, wspiera wybór użytkownika, kontrolę użytkownika i wzmacnia pozycję użytkownika.

Osoby fizyczne korzystające z przysługującego im prawa dostępu przyznanego na mocy dyrektywy o ochronie danych 95/46/WE nie miały wpływu na format, w którym administrator danych postanowił przekazać żądane informacje. **Nowe prawo do przenoszenia danych ma na celu wzmocnienie pozycji osób, których dane dotyczą, w stosunku do ich własnych danych osobowych, ponieważ ułatwia ono tym osobom przenoszenie, kopiowanie lub przekazywanie danych osobowych między środowiskami IT** (bez względu na to, czy chodzi o ich własne systemy, systemy zaufanej osoby trzeciej lub systemy nowych administratorów danych).

Poprzez potwierdzenie praw osobistych osób fizycznych i sprawowanie kontroli nad danymi osobowymi ich dotyczącymi, przenoszenie danych stanowi również szansę na „przywrócenie równowagi" w stosunkach między osobami, których dane dotyczą, i administratorami danych[1].

Prawo do przenoszenia danych osobowych może też wzmocnić konkurencję między usługami (poprzez ułatwienie zmiany usługodawcy), jednak RODO reguluje dane osobowe, nie konkurencję. W szczególności w art. 20 nie ogranicza się danych podlegających przeniesieniu do tych danych, które są niezbędne lub użyteczne przy zmianie usługodawcy[2].

Chociaż przenoszenie danych jest nowym prawem, inne sposoby przenoszenia już istnieją lub są omawiane w innych dziedzinach prawodawstwa (np. w kontekstach rozwiązania umowy, roamingu w usługach komunikacyjnych i transgranicznego dostępu do usług[3]). Między poszczególnymi rodzajami przenoszenia mogą powstać synergie, a nawet korzyści dla osób fizycznych, jeżeli świadczy się je, przyjmując podejście łączone. Do analogii należy jednak podchodzić z ostrożnością.

W opinii tej przedstawiono wytyczne dla administratorów danych, aby mogli oni zaktualizować swoje praktyki, procedury i politykę, a także wyjaśniono w niej znaczenie przenoszenia danych, aby dać osobom, których dane dotyczą, możliwość efektywnego wykorzystania ich nowego prawa.

[1] Głównym celem przenoszenia danych jest wzmocnienie kontroli osoby fizycznej nad jej danymi osobowymi i zapewnienie tej osobie czynnej roli w ekosystemie danych.
[2] Np. prawo to może umożliwić bankom świadczenie dodatkowych usług – kontrolowanych przez użytkownika – przy wykorzystaniu danych osobowych zebranych początkowo w ramach świadczenia usługi dostaw energii.
[3] Zob. agenda jednolitego rynku cyfrowego Komisji Europejskiej: https://ec.europa.eu/digital-agenda/en/digital-single-market, w szczególności pierwszy filar polityki: „Lepszy dostęp do towarów i usług internetowych".

II. Jakie są główne elementy przenoszenia danych?

W art. 20 ust. 1 RODO prawo do przenoszenia danych zdefiniowano w następujący sposób:

> *Osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła administratorowi, oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe [...]*

- **Prawo do otrzymania danych osobowych**

Po pierwsze, przenoszenie danych jest **prawem osoby, której dane dotyczą, do otrzymania podzbioru danych osobowych** jej dotyczących przetworzonych przez administratora danych oraz do przechowywania tych danych do dalszego użytku osobistego. Dane można przechowywać na prywatnym urządzeniu lub w prywatnej chmurze, bez konieczności przekazywania ich innemu administratorowi danych.

Pod tym względem przenoszenie danych uzupełnia prawo dostępu. Swoistością przenoszenia danych jest fakt, że daje ono osobom, których dane dotyczą, możliwość łatwego osobistego zarządzania i ponownego wykorzystania danych osobowych. Te dane należy przekazać w „ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego". Na przykład osoba, której dane dotyczą, może być zainteresowana uzyskaniem swojej obecnej listy odtwarzania (lub historii słuchanych utworów) z serwisu strumieniowej transmisji muzyki, aby sprawdzić, ile razy odsłuchała konkretnych utworów lub sprawdzić, które utwory chce zakupić lub których utworów chce posłuchać na innej platformie. W podobny sposób osoba ta może również chcieć uzyskać swoją listę kontaktów z aplikacji webmail, np. aby stworzyć listę gości weselnych, uzyskać informacje na temat zakupów dokonanych przy użyciu różnych kart lojalnościowych lub ocenić swój ślad węglowy[4].

- **Prawo do przesyłania danych osobowych przez jednego administratora danych innemu administratorowi**

Po drugie, art. 20 ust. 1 nadaje osobom, których dane dotyczą, **prawo do przesyłania danych osobowych przez jednego administratora danych innemu administratorowi** „bez przeszkód". Na żądanie osoby, której dane dotyczą, administrator danych może również przesłać dane bezpośrednio innemu administratorowi danych, o ile jest to technicznie możliwe (art. 20 ust. 2). W tym zakresie w motywie 68 zachęca się administratorów danych do opracowywania interoperacyjnych formatów, które umożliwiają przenoszenie danych[5], nie nakładając jednak na administratorów obowiązku prowadzenia lub wprowadzenia

[4] W tych przypadkach przetworzenie danych przez osobę, której dane dotyczą, może mieć miejsce w ramach działalności domowej – jeżeli przetwarzanie jest w całości kontrolowane przez osobę, której dane dotyczą – albo przetworzenia w imieniu osoby, której dane dotyczą, może podjąć się osoba trzecia. W tej drugiej sytuacji wspomnianą osobę trzecią należy uznać za administratora danych nawet w przypadku wyłącznego celu przechowywania danych osobowych, w związku z czym ta osoba trzecia musi przestrzegać zasad i obowiązków określonych w RODO.
[5] Zob. również sekcja V.

kompatybilnych technicznie systemów przetwarzania[6]. W RODO nie zakazano jednak administratorom tworzenia barier utrudniających przesyłanie.

Zasadniczo ten element przenoszenia danych zapewnia osobom, których dane dotyczą, możliwość nie tylko uzyskania i ponownego wykorzystania, ale również przesyłania danych, które dostarczyły one innemu usługodawcy (w ramach tego samego sektora przedsiębiorstw albo w innym sektorze). Oczekuje się, że oprócz wzmocnienia pozycji konsumenta poprzez zapobieżenie uzależnieniu od jednego dostawcy prawo do przenoszenia danych będzie sprzyjać innowacji i wymianie danych osobowych między administratorami danych w sposób bezpieczny i pewny, pod kontrolą osoby, której dane dotyczą[7]. Przenoszenie danych może wspierać kontrolowaną i ograniczoną wymianę danych osobowych przez użytkowników między organizacjami i w ten sposób wzbogacić usługi i doświadczenia konsumentów[8]. Przenoszenie danych może ułatwić przesyłanie oraz ponowne wykorzystywanie danych osobowych dotyczących użytkowników w ramach różnych usług, którymi są oni zainteresowani.

[6] W związku z tym należy zwracać szczególną uwagę na format przesyłanych danych w celu zapewnienia, by dane mogły zostać z łatwością ponownie wykorzystane przez osobę, której dane dotyczą, lub przez innego administratora danych. Zob. również sekcja V.

[7] Zob. szereg eksperymentalnych aplikacji w Europie, na przykład aplikacja MiData w Wielkiej Brytanii, aplikacje MesInfos/SelfData stworzone przez FING we Francji.

[8] Sektory tzw. „mierzenia siebie" (ang. *quantified self*) i internetu rzeczy wykazały korzyści (i zagrożenia) związane z łączeniem danych osobowych z różnych aspektów życia danej osoby fizycznej, takich jak sprawność fizyczna, aktywność i liczba spożywanych kalorii, celem tworzenia pełniejszego obrazu życia tej osoby w jednym pliku.

- **Administrowanie**

Przenoszenie danych zapewnia prawo do otrzymywania danych osobowych oraz ich przetwarzania zgodnie z wolą osoby, której dane dotyczą[9].

Administratorzy danych odpowiadający na żądania przeniesienia danych – na warunkach określonych w art. 20 – nie są odpowiedzialni za przetwarzanie dokonywane przez osobę, której dane dotyczą, lub przez inne przedsiębiorstwo otrzymujące dane osobowe. Działają oni w imieniu osoby, której dane dotyczą, w tym wówczas, gdy dane osobowe są przesyłane bezpośrednio innemu administratorowi danych. W tym względzie administrator danych nie ponosi odpowiedzialności za przestrzeganie prawa ochrony danych przez otrzymującego administratora danych, biorąc pod uwagę fakt, że to nie wysyłający administrator danych wybiera odbiorcę. Jednocześnie administrator powinien ustanowić gwarancje w celu zapewnienia, by rzeczywiście działał on w imieniu osoby, której dane dotyczą. Przykładowo może on ustanowić procedury w celu zapewnienia, by rodzaj przesyłanych danych osobowych pokrywał się faktycznie z rodzajem danych, jaki osoba, której dane dotyczą, pragnie przesłać. Można osiągnąć ten cel poprzez uzyskanie potwierdzenia od osoby, której dane dotyczą, przed przesłaniem albo na wcześniejszym etapie – w chwili udzielania pierwotnej zgody na przetwarzanie lub finalizacji umowy.

Na administratorach danych odpowiadających na żądanie przeniesienia danych nie ciąży szczególny obowiązek sprawdzania i weryfikacji jakości danych przed ich przesłaniem. Nie ulega wątpliwości, że dane te powinny być już prawidłowe i aktualne zgodnie z zasadami określonymi w art. 5 ust. 1 RODO. Ponadto przenoszenie danych nie nakłada na administratora danych obowiązku zatrzymywania danych osobowych dłużej niż jest to konieczne ani po upływie wyznaczonego okresu zatrzymania[10]. Co istotne, nie istnieje dodatkowy wymóg zatrzymania danych po upływie okresów mających zazwyczaj zastosowanie, aby można je było wykorzystać do celów wszelkich potencjalnych przyszłych żądań przeniesienia danych.

Gdy dane osobowe objęte żądaniem są przetwarzane przez przetwarzającego, umowa zawarta zgodnie z art. 28 RODO musi zawierać obowiązek pomocy „administratorowi poprzez odpowiednie środki techniczne i organizacyjne, […] [aby] wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw". Administrator danych powinien zatem wdrożyć określone procedury we współpracy ze swoimi przetwarzającymi, aby odpowiedzieć na żądania przeniesienia danych. W przypadku wspólnego administrowania w umowie należy jednoznacznie rozdzielić między wszystkich administratorów danych obowiązki dotyczące przetwarzania żądań przeniesienia danych.

Ponadto otrzymujący administrator danych[11] jest odpowiedzialny za zapewnienie, by dostarczone dane podlegające przenoszeniu były stosowne i nie były nadmierne w odniesieniu do nowego przetwarzania danych. Przykładowo w przypadku żądania przeniesienia danych wniesionego do dostawcy aplikacji *webmail*, w ramach którego osoba, której dane dotyczą, wykorzystuje wniesione żądanie w celu uzyskania wiadomości e-mail i przesłania ich na

[9] Prawo do przenoszenia danych nie jest ograniczone do danych osobowych, które są przydatne i stosowne w odniesieniu do podobnych usług świadczonych przez konkurentów administratora danych.

[10] W powyższym przykładzie, jeżeli administrator danych nie zatrzymuje listy utworów muzycznych odtwarzanych przez użytkownika, nie można zawrzeć tych danych osobowych w żądaniu przeniesienia danych.

[11] Tj. administrator danych, który otrzymuje dane osobowe po wniesieniu przez osobę, której dane dotyczą, żądania przeniesienia danych do innego administratora danych.

zabezpieczoną platformę służącą archiwizacji, nowy administrator danych nie musi przetwarzać danych kontaktowych korespondentów osoby, której dane dotyczą. Jeżeli informacje te nie są stosowne w odniesieniu do celu nowego przetwarzania, nie należy ich przechowywać ani przetwarzać. W każdym przypadku otrzymujący administratorzy danych nie są zobowiązani do przyjmowania i przetwarzania danych osobowych przesłanych w następstwie żądania przeniesienia danych. Podobnie w przypadku, gdy osoba, której dane dotyczą, żąda przesłania informacji dotyczących jej transakcji bankowych do usługi, która pomaga jej w zarządzaniu budżetem, otrzymujący administrator danych nie musi przyjmować wszystkich danych ani zachowywać wszystkich informacji szczegółowych dotyczących transakcji po ich oznaczeniu do celów nowej usługi. Innymi słowy, przyjęte i zatrzymane dane powinny obejmować wyłącznie dane niezbędne i stosowne w odniesieniu do usługi świadczonej przez otrzymującego administratora danych.

Organizacja „otrzymująca" staje się nowym administratorem danych w odniesieniu do tych danych osobowych i musi przestrzegać zasad określonych w art. 5 RODO. W związku z tym „nowy" otrzymujący administrator danych musi jednoznacznie i bezpośrednio określić cel nowego przetwarzania przed wniesieniem jakiegokolwiek żądania przeniesienia danych podlegających przenoszeniu zgodnie z wymogami przejrzystości określonymi w art. 14[12]. Podobnie jak w przypadku wszystkich innych czynności przetwarzania danych, za które odpowiada administrator danych, powinien on stosować zasady ustanowione w art. 5, takie jak zgodność z prawem, rzetelność i przejrzystość, ograniczenie celu, minimalizacja danych, prawidłowość, integralność i poufność, ograniczenie przechowywania oraz rozliczalność[13].

Administratorzy danych przechowujący dane osobowe powinni być przygotowani do ułatwienia osobie, której dane dotyczą, wykonania przysługującego jej prawa do przenoszenia danych. Administratorzy danych mogą również zdecydować o przyjęciu danych od osoby, której dane dotyczą, ale nie są do tego zobowiązani.

- **Przenoszenie danych a inne prawa osób, których dane dotyczą**

Wykonanie przez osobę fizyczną przysługującego jej prawa do przenoszenia danych (lub wszelkich innych praw określonych w RODO) pozostaje bez uszczerbku dla wszelkich innych praw. Osoba, której dane dotyczą, może nadal korzystać z usług administratora danych nawet po zakończeniu operacji przenoszenia danych. Przenoszenie danych nie powoduje automatycznego usunięcia danych[14] z systemów administratora danych i pozostaje bez uszczerbku dla pierwotnego okresu zatrzymania mającego zastosowanie do danych, które przesłano. Osoba, której dane dotyczą, może korzystać ze swoich praw, o ile administrator danych nadal przetwarza dane.

Podobnie, jeżeli osoba, której dane dotyczą, pragnie wykonać przysługujące jej prawo do usunięcia danych („prawo do bycia zapomnianym" określone w art. 17), administrator danych

[12] Ponadto nowy administrator danych nie powinien przetwarzać danych osobowych, które nie są istotne, przy czym przetwarzanie musi być ograniczone do tego, co jest niezbędne do nowych celów, nawet jeżeli dane osobowe stanowią część bardziej globalnej bazy danych przesyłanych w ramach procedury przenoszenia. Dane osobowe, które nie są niezbędne do osiągnięcia celu nowego przetwarzania, należy jak najszybciej usunąć.

[13] Po otrzymaniu danych osobowych przez administratora danych dane osobowe przesłane w ramach wykonania prawa do przenoszenia danych można uznać za „dostarczone przez" osobę, której dane dotyczą, i ponownie je przesłać zgodnie z prawem do przenoszenia danych w zakresie, w jakim spełnione są pozostałe warunki umożliwiające wykonanie tego prawa (tj. podstawa prawna przetwarzania itd.).

[14] Jak wskazano w art. 17 RODO.

nie może wykorzystać przenoszenia danych jako sposobu opóźnienia lub odmowy takiego usunięcia.

Jeżeli osoba, której dane dotyczą, odkryje, że dane osobowe żądane w wykonaniu prawa do przenoszenia danych nie odpowiadają w pełni jej żądaniu, każde kolejne żądanie dostępu do danych osobowych w wykonaniu prawa dostępu należy spełnić w całości, zgodnie z art. 15 RODO.

Ponadto w przypadku, gdy w przepisach szczególnych innej gałęzi prawa europejskiego lub prawa państwa członkowskiego również przewiduje się pewną formę przenoszenia przedmiotowych danych, podczas spełniania żądania przeniesienia danych zgodnie z RODO należy uwzględnić również warunki określone w tego rodzaju przepisach szczególnych. Po pierwsze, jeżeli z żądania wniesionego przez osobę, której dane dotyczą, bezsprzecznie wynika, że jej zamiarem nie jest wykonanie uprawnień przewidzianych w RODO, lecz wyłącznie wykonanie uprawnień przewidzianych w przepisach sektorowych, przepisy RODO dotyczące przenoszenia danych nie będą miały zastosowania do tego żądania[15]. Jeżeli natomiast celem żądania jest przeniesienie na mocy RODO, istnienie tego rodzaju przepisów szczególnych nie powoduje uchylenia ogólnej zasady przenoszenia danych stosowanej wobec wszystkich administratorów danych, jak przewidziano w RODO. Zamiast tego należy ocenić w poszczególnych przypadkach, w jaki sposób, o ile w ogóle, tego rodzaju przepisy szczególne mogą wpłynąć na prawo do przenoszenia danych.

III. W jakich sytuacjach ma zastosowanie przenoszenie danych?

- **Które operacje przetwarzania są objęte prawem do przenoszenia danych?**

Aby zachować zgodność z RODO, administratorzy danych muszą mieć wyraźną podstawę prawną do przetwarzania danych osobowych.

Zgodnie z art. 20 ust. 1 lit. a) RODO, **aby wchodzić w zakres przenoszenia danych**, operacje przetwarzania muszą się odbywać:

- na podstawie zgody osoby, której dane dotyczą (w myśl art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a), jeżeli chodzi o szczególne kategorie danych osobowych);

- albo na podstawie umowy, której stroną jest osoba, której dane dotyczą, w myśl art. 6 ust. 1 lit. b).

W ramach przykładu: tytuły książek nabytych przez osobę fizyczną w księgarni internetowej lub utwory muzyczne słuchane za pośrednictwem serwisu transmisji strumieniowej muzyki stanowią przykład danych osobowych, które co do zasady są objęte zakresem przenoszenia danych, ponieważ są przetwarzane na podstawie wykonywania umowy, której stroną jest osoba, której dane dotyczą.

[15] Przykładowo, jeżeli żądanie osoby, której dane dotyczą, ma w szczególności na celu zapewnienie dostępu do historii jej rachunku bankowego dostawcy świadczącemu usługę dostępu do informacji o rachunku do celów wskazanych w drugiej dyrektywie w sprawie usług płatniczych, tego rodzaju dostęp należy zapewnić zgodnie z przepisami tej dyrektywy.

W RODO nie ustanowiono ogólnego prawa do przenoszenia danych w przypadkach, w których przetwarzanie danych osobowych nie odbywa się na podstawie zgody lub umowy[16]. Przykładowo instytucje finansowe nie są zobowiązane do udzielenia odpowiedzi na żądania przeniesienia danych dotyczące danych osobowych przetwarzanych w wykonaniu ciążących na nich obowiązków w zakresie zapobiegania praniu pieniędzy i jego wykrywania, a także zapobiegania innym przestępstwom finansowych oraz ich wykrywania; podobnie przenoszenie danych nie obejmuje zawodowych danych kontaktowych przetwarzanych w relacji między przedsiębiorcami w przypadkach, gdy przetwarzanie nie opiera się ani na zgodzie osoby, której dane dotyczą, ani na umowie, której jest ona stroną.

Jeżeli chodzi o dane pracowników, prawo do przenoszenia danych ma co do zasady zastosowanie wyłącznie wówczas, gdy przetwarzanie opiera się na umowie, której stroną jest osoba, której dane dotyczą. W wielu przypadkach zgoda nie będzie w tym kontekście uznana za wyrażoną dobrowolnie ze względu na brak równowagi sił między pracodawcą a pracownikiem[17]. Niektóre operacje przetwarzania w kontekście zasobów ludzkich oparte są natomiast na podstawie prawnej w postaci prawnie uzasadnionego interesu lub są konieczne do zapewnienia wykonania określonych zobowiązań prawnych w obszarze zatrudnienia. W praktyce nie ulega wątpliwości, że prawo do przenoszenia danych w kontekście zasobów ludzkich dotyczyć będzie określonych operacji przetwarzania (takich jak usługi w zakresie płac i wynagrodzeń, wewnętrzna rekrutacja), ale w wielu innych sytuacjach potrzebne będzie przyjęcie indywidualnego podejścia, aby sprawdzić, czy spełnione są wszystkie warunki mające zastosowanie do prawa do przenoszenia danych.

Ponadto prawo do przenoszenia danych ma zastosowanie wyłącznie wówczas, gdy przetwarzanie danych „odbywa się w sposób zautomatyzowany", i w związku z tym nie obejmuje większości dokumentów w formie papierowej.

- **Które dane osobowe należy uwzględnić?**

Zgodnie z art. 20 ust. 1, aby dane były objęte zakresem prawa do przenoszenia danych:
- muszą to być dane osobowe dotyczące danej osoby; oraz
- muszą to być dane, które *dostarczyła* ona administratorowi danych.

Art. 20 ust. 4 stanowi również, że wykonanie tego prawa nie może niekorzystnie wpływać na prawa i wolności innych.

Pierwszy warunek: dane osobowe dotyczące osoby, której dane dotyczą

[16] Zob. motyw 68 i art. 20 ust. 3 RODO. W art. 20 ust. 3 i w motywie 68 przewidziano, że przenoszenie danych nie ma zastosowania do przetwarzania danych, jeżeli jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi lub jeżeli administrator danych wykonuje obowiązki publiczne lub wywiązuje się z obowiązku prawnego.
W przytoczonych przypadkach administratorzy danych nie mają zatem obowiązku zapewniania przenoszenia danych. Dobrą praktyką jest jednak opracowanie procedur automatycznego odpowiadania na żądania przeniesienia, z poszanowaniem zasad regulujących prawo do przenoszenia danych. Przykładem tego rodzaju praktyki byłby serwis rządowy zapewniający łatwe pobieranie poprzednio złożonych deklaracji podatkowych dotyczących podatku dochodowego od osób fizycznych. W odniesieniu do przenoszenia danych jako dobrej praktyki w przypadku przetwarzania opartego na podstawie prawnej w postaci konieczności prawnie uzasadnionego interesu oraz istniejących programów dobrowolnych – zob. s. 47 i 48 opinii Grupy Roboczej Art. 29 6/2014 w sprawie pojęcia prawnie uzasadnionych interesów (WP 217).
[17] Jak wskazała Grupa Robocza Art. 29 w opinii 8/2001 z dnia 13 września 2001 r. (WP 48).

Zakresem żądania przeniesienia danych objęte są wyłącznie dane osobowe. W związku z tym wszelkie dane anonimowe[18] lub nieodnoszące się do osoby, której dane dotyczą, nie będą objęte tym zakresem. Dane pseudonimiczne, które można jednoznacznie powiązać z osobą, której dane dotyczą (np. poprzez podanie przez nią odpowiedniego identyfikatora, por. art. 11 ust. 2), są jednak tym zakresem objęte.

W wielu sytuacjach administratorzy danych przetwarzają informacje zawierające dane osobowe kilku osób, których dane dotyczą. W takim przypadku administratorzy danych nie powinni dokonywać zbyt zawężającej wykładni określenia „dane osobowe dotyczące osoby, której dane dotyczą". Przykładowo rejestry połączeń telefonicznych, wiadomości interpersonalnych lub VoIP (w historii konta abonenta) mogą zawierać dane osób trzecich uczestniczących w połączeniach przychodzących i wychodzących. Chociaż rejestry będą w związku z tym zawierały dane osobowe dotyczące wielu osób, abonenci powinni mieć możliwość otrzymania tych rejestrów w odpowiedzi na żądania przeniesienia danych, ponieważ rejestry dotyczą (również) osoby, której dane dotyczą. Jeżeli tego rodzaju rejestry zostają następnie przesłane nowemu administratorowi danych, nie powinien on ich jednak przetwarzać w żadnym celu, który wpłynąłby niekorzystnie na prawa i wolności osób trzecich (zob. poniżej: trzeci warunek).

Drugi warunek: dane dostarczone przez osobę, której dane dotyczą

Drugi warunek zawęża omawiany zakres do danych „dostarczonych przez" osobę, której dane dotyczą.

Istnieje wiele przykładów danych osobowych świadomie i aktywnie „dostarczanych przez" osobę, której dane dotyczą, takie jak dane dotyczące konta (np. adres e-mail, nazwa użytkownika, wiek) podawane w formularzach *online*. Dane „dostarczone przez" osobę, której dane dotyczą, wynikają jednak również z obserwacji jej działań. W związku z tym Grupa Robocza Art. 29 uważa, że aby nadać pełną wartość temu nowemu prawu, określenie „dostarczone przez" powinno obejmować również dane osobowe wynikające z obserwacji działań użytkowników, takie jak dane pierwotne przetwarzane przez inteligentny licznik lub inne rodzaje połączonych obiektów[19], dzienniki aktywności, historia korzystania ze strony internetowej lub czynności wyszukiwania.

Ta ostatnia kategoria danych nie obejmuje danych wytwarzanych przez administratora danych (z wykorzystaniem zaobserwowanych danych lub danych bezpośrednio dostarczonych jako dane wejściowe), takich jak profil użytkownika utworzony poprzez analizę danych pierwotnych zgromadzonych za pośrednictwem inteligentnego pomiaru.

Można wyróżnić różne kategorie danych w zależności od ich pochodzenia, aby określić, czy są one objęte prawem do przenoszenia danych. Następujące kategorie danych można zaklasyfikować jako „dostarczone przez osobę, której dane dotyczą":

[18] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_pl.pdf
[19] Dzięki możliwości uzyskania danych wynikających z obserwacji jej działań, osoba, której dane dotyczą, będzie również mogła uzyskać lepszy obraz wyborów dotyczących wdrażania dokonywanych przez administratora danych w odniesieniu do zakresu obserwowanych danych i znajdzie się w korzystniejszej sytuacji, jeżeli chodzi o wybór danych, jakie jest gotowa dostarczyć, aby uzyskać podobną usługę, a także będzie świadoma stopnia, w jakim przestrzegane jest jej prawo do prywatności.

- **dane aktywnie i świadomie dostarczone przez osobę, której dane dotyczą** (na przykład adres e-mail, nazwa użytkownika, wiek itd.);
- **zaobserwowane dane dostarczone przez osobę, której dane dotyczą, poprzez korzystanie z danej usługi lub danego urządzenia.** Mogą one na przykład obejmować historię wyszukiwania danej osoby, dane o ruchu i dane dotyczące lokalizacji. Mogą również obejmować inne dane pierwotne, takie jak tętno monitorowane za pośrednictwem urządzenia do noszenia na ciele.

Dane wywnioskowane i dane wywiedzione są natomiast wytwarzane przez administratora danych na podstawie danych „dostarczonych przez osobę, której dane dotyczą". Przykładowo wyniku oceny zdrowia użytkownika lub profilu utworzonego w kontekście zarządzania ryzykiem i regulacji finansowych (np. w celu przypisania punktów w ramach punktowej oceny kredytowej lub przestrzegania przepisów dotyczących przeciwdziałania praniu pieniędzy) nie można jako takich uznać za „dostarczone przez" osobę, której dane dotyczą. Chociaż tego rodzaju dane mogą stanowić część profilu zarządzanego przez administratora danych i zostały one wywnioskowane lub wywiedzione z analizy danych dostarczonych przez osobę, której dane dotyczą (na przykład poprzez jej działania), co do zasady nie zostaną one uznane za „dostarczone przez osobę, której dane dotyczą", i tym samym nie będą objęte zakresem tego nowego prawa[20].

Co do zasady, biorąc pod uwagę cele polityczne prawa do przenoszenia danych, należy dokonywać wykładni rozszerzającej określenia „dostarczone przez osobę, której dane dotyczą" i należy wyłączyć z jego zakresu „dane wywnioskowane" i „dane wywiedzione" obejmujące dane osobowe utworzone przez usługodawcę (na przykład wyniki algorytmiczne). Administrator danych może wyłączyć te wywnioskowane dane, jednak powinien uwzględnić wszystkie inne dane osobowe dostarczone przez osobę, której dane dotyczą, za pośrednictwem środków technicznych zapewnionych przez administratora[21].

Określenie „dostarczone przez" obejmuje zatem dane osobowe odnoszące się do działania osoby, której dane dotyczą, lub wyniku obserwacji zachowania określonej osoby fizycznej, lecz nie obejmuje danych wynikających z późniejszej analizy tego zachowania. Wszelkie dane osobowe wytworzone przez administratora danych w ramach przetwarzania danych, np. w procesie personalizacji lub rekomendacji, kategoryzację użytkownika lub jego profilowanie, stanowią dane wywiedzione lub wywnioskowane z danych osobowych dostarczonych przez osobę, której dane dotyczą, przy czym nie są one objęte prawem do przenoszenia danych.

Trzeci warunek: prawo do przenoszenia danych nie może niekorzystnie wpływać na prawa i wolności innych

[20] Osoba, której dane dotyczą, jest jednak nadal „uprawniona do uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz następujących informacji" oraz informacji „o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą", zgodnie z art. 15 RODO (który dotyczy prawa dostępu).

[21] Obejmują one wszystkie dane na temat osoby, której dane dotyczą, zaobserwowane podczas działań, do celów których dane te są gromadzone, takie jak historia transakcji lub dziennik dostępu. Dane zgromadzone poprzez śledzenie i rejestrowanie osoby, której dane dotyczą (np. za pośrednictwem aplikacji rejestrującej tętno lub technologii wykorzystywanej w celu śledzenia zachowania dotyczącego przeglądania), również należy uznać za „dostarczone przez" tę osobę, nawet jeżeli dane te nie zostały przesłane aktywnie lub świadomie.

W odniesieniu do danych osobowych dotyczących innych osób, których dane dotyczą:

Trzeci warunek ma na celu uniknięcie uzyskiwania danych obejmujących dane osobowe innych osób, których dane dotyczą (które nie wyraziły odpowiedniej zgody), oraz przesyłania takich danych nowemu administratorowi danych w przypadkach, gdy istnieje prawdopodobieństwo, że dane te będą przetwarzane w sposób, który wpływałby niekorzystnie na prawa i wolności pozostałych osób, których dane dotyczą (art. 20 ust. 4 RODO)[22].

Tego rodzaju niekorzystny wpływ miałby miejsce na przykład wówczas, gdy przesyłanie danych przez jednego administratora danych innemu administratorowi uniemożliwia osobom trzecim wykonywanie uprawnień przysługujących im jako osobom, których dane dotyczą, na mocy RODO (np. prawa do informacji, prawa dostępu itd.).

Osoba, której dane dotyczą, inicjująca przesyłanie swoich danych innemu administratorowi danych, udziela zgody na przetwarzanie danych nowemu administratorowi danych albo zawiera umowę z tym administratorem. Jeżeli dane osobowe osób trzecich są zawarte w zbiorze danych, należy określić inną podstawę prawną przetwarzania. Przykładowo prawnie uzasadniony interes może być realizowany przez administratora danych na mocy art. 6 ust. 1 lit. f), w szczególności gdy celem administratora danych jest świadczenie usługi na rzecz osoby, której dane dotyczą, a usługa ta umożliwia wspomnianej osobie przetwarzanie danych osobowych w ramach czynności o czysto osobistym lub domowym charakterze. Operacje przetwarzania zainicjowane przez osobę, której dane dotyczą, w kontekście czynności o charakterze osobistym, które dotyczą osób trzecich i potencjalnie wywierają na nie wpływ, należą do zakresu odpowiedzialności tej osoby w stopniu, w jakim o takim przetwarzaniu nie decyduje w jakikolwiek sposób administrator danych.

Przykładowo usługa *webmail* może umożliwić utworzenie spisu kontaktów, znajomych, krewnych, członków rodziny i szerszego otoczenia osoby, której dane dotyczą. Ponieważ dane te dotyczą możliwej do zidentyfikowania osoby fizycznej, która pragnie wykonać przysługujące jej prawo do przenoszenia danych (i są wytwarzane przez tę osobę), administratorzy danych powinni przesłać cały spis przychodzących i wychodzących wiadomości e-mail tej osobie, której dane dotyczą.

Podobnie rachunek bankowy osoby, której dane dotyczą, może zawierać dane osobowe dotyczące transakcji dokonywanych nie tylko przez posiadacza rachunku, ale również przez inne osoby fizyczne (np. jeżeli przekazały one środki pieniężne posiadaczowi rachunku). Jest mało prawdopodobne, by przesłanie informacji dotyczących rachunku bankowego posiadaczowi rachunku niekorzystnie wpłynęło na prawa i wolności tych osób trzecich po wniesieniu żądania przeniesienia – pod warunkiem, że w obu przykładach dane są wykorzystywane w tym samym celu (tj. adres kontaktowy wykorzystywany wyłącznie przez osobę, której dane dotyczą, lub historia rachunku bankowego osoby, której dane dotyczą).

Prawa i wolności osób trzecich zostaną natomiast naruszone, jeżeli nowy administrator danych wykorzysta dane osobowe do innych celów, np. jeżeli otrzymujący administrator danych wykorzysta dane osobowe innych osób fizycznych figurujących w spisie kontaktów osoby, której dane dotyczą, do celów marketingowych.

[22] Motyw 68 stanowi, że „jeżeli określony zestaw danych osobowych odnosi się do więcej niż jednej osoby, której dane dotyczą, prawo do otrzymania danych osobowych nie powinno powodować uszczerbku dla praw i wolności innych osób, których dane dotyczą, na podstawie niniejszego rozporządzenia".

W związku z tym, aby zapobiec wywarciu niekorzystnego wpływu na zaangażowane osoby trzecie, przetwarzanie takich danych osobowych przez innego administratora jest dopuszczalne wyłącznie w zakresie, w jakim dane są przechowywane pod wyłączną kontrolą użytkownika wnoszącego żądanie i są zarządzane wyłącznie w celu zaspokojenia potrzeb o czysto osobistym lub domowym charakterze. Otrzymujący „nowy" administrator danych (któremu dane mogą zostać przesłane na żądanie użytkownika) nie może wykorzystywać przesłanych danych osób trzecich do własnych celów, np. w celu oferowania produktów i usług marketingowych tym innym osobom, których dane dotyczą, będącym osobami trzecimi. Przykładowo informacji tych nie należy wykorzystywać do wzbogacenia profilu osoby trzeciej, której dane dotyczą, oraz do odbudowy jej środowiska społecznego, bez jej wiedzy i zgody[23]. Nie można ich również wykorzystywać w celu uzyskania informacji na temat takich osób trzecich oraz tworzenia określonych profili, nawet jeżeli ich dane osobowe znajdują się już w posiadaniu administratora danych. W przeciwnym razie istnieje prawdopodobieństwo, że takie przetwarzanie będzie niezgodne z prawem i nieuczciwe, w szczególności jeżeli osoby trzecie, których sprawa dotyczy, nie są o tym poinformowane i nie mogą wykonywać uprawnień przysługujących im jako osobom, których dane dotyczą.

Ponadto dominującą praktyką w przypadku wszystkich administratorów danych (zarówno stron „przesyłających", jak i „otrzymujących") jest wdrażanie narzędzi umożliwiających osobom, których dane dotyczą, wybór istotnych danych, które pragną otrzymać i przesłać, oraz wyłączenie – w stosownych przypadkach – danych innych osób fizycznych. Praktyka ta w dalszym stopniu przyczyni się do ograniczenia zagrożeń dla osób trzecich, których dane osobowe mogą zostać przeniesione.

Ponadto administratorzy danych powinni wdrożyć mechanizmy zgody w odniesieniu do innych zaangażowanych osób, których dane dotyczą, aby ułatwić przesyłanie danych w przypadkach, gdy takie osoby są gotowe wyrazić zgodę, np. jeżeli również pragną przenieść swoje dane do innego administratora danych. Taka sytuacja może mieć miejsce na przykład w przypadku portali społecznościowych, jednak decyzja dotycząca wyboru dominującej praktyki pozostaje w gestii administratorów danych.

W odniesieniu do danych objętych prawem własności intelektualnej i tajemnicami handlowymi:
O prawach i wolnościach innych wspomniano w art. 20 ust. 4. Chociaż nie są one bezpośrednio związane z przenoszeniem, można je rozumieć jako „[obejmujące] tajemnice handlowe lub własność intelektualną, w szczególności [...] prawa autorskie chroniące oprogramowanie". Chociaż prawa te należy uwzględnić przed udzieleniem odpowiedzi na żądanie przeniesienia danych, „względy te nie powinny jednak skutkować odmową udzielenia osobie, której dane dotyczą, jakichkolwiek informacji". Ponadto administrator danych nie powinien odrzucać żądania przeniesienia danych ze względu na naruszenie innego prawa wynikającego z umowy (na przykład ze względu na niespłacony dług lub konflikt handlowy z osobą, której dane dotyczą).

[23] Serwis społecznościowy nie powinien wzbogacać profili swoich członków, wykorzystując dane osobowe przesłane przez osobę, której dane dotyczą, w wykonaniu przysługującego jej prawa do przenoszenia danych, nie przestrzegając zasady przejrzystości oraz nie upewniwszy się, że opiera się on na odpowiedniej podstawie prawnej w zakresie tego konkretnego przetwarzania.

Ponadto prawo do przenoszenia danych nie jest prawem danej osoby fizycznej do nadużywania informacji w sposób, który można by zaklasyfikować jako nieuczciwą praktykę lub który stanowiłby naruszenie praw własności intelektualnej.

Potencjalne ryzyko biznesowe nie może jednak samo w sobie stanowić podstawy do odmowy udzielenia odpowiedzi na żądanie przeniesienia, przy czym administratorzy danych mogą przesłać dane osobowe dostarczone przez osoby, których dane dotyczą, w formie, która nie ujawnia informacji objętych tajemnicami handlowymi lub prawami własności intelektualnej.

IV. W jaki sposób do przenoszenia danych stosuje się przepisy ogólne regulujące wykonywanie praw przysługujących osobie, której dane dotyczą,?

- **Jakie informacje należy uprzednio przekazać osobie, której dane dotyczą?**

W celu zapewnienia zgodności z nowym prawem do przenoszenia danych administratorzy danych muszą informować osoby, których dane dotyczą, o istnieniu nowego prawa do przenoszenia danych. Jeżeli dane osobowe, których sprawa dotyczy, są bezpośrednio zbierane od osoby, której dane dotyczą, informacje te należy podać „podczas pozyskiwania danych osobowych". Jeżeli danych osobowych nie pozyskano od osoby, której dane dotyczą, administrator danych musi przekazać osobie, której dane dotyczą, informacje określone w art. 13 ust. 2 lit. b) i art. 14 ust. 2 lit. c).

„Jeżeli danych osobowych nie pozyskano od osoby, której dane dotyczą", zgodnie z art. 14 ust. 3 informacje należy podać w rozsądnym terminie nieprzekraczającym jednego miesiąca od dnia pozyskania danych osobowych, przy pierwszej komunikacji z osobą, której dane dotyczą, lub w przypadku ujawnienia danych osobom trzecim[24].

Przekazując wymagane informacje, administratorzy danych muszą zapewnić, że odróżniają prawo do przenoszenia danych od innych praw. W związku z tym Grupa Robocza Art. 29 zaleca w szczególności, aby administratorzy danych wyraźnie wyjaśnili różnicę między rodzajami danych, jakie osoba, których dane dotyczą, może otrzymać na mocy przysługującego jej prawa dostępu i prawa do przenoszenia danych.

Ponadto Grupa Robocza zaleca, aby administratorzy danych zawsze przekazywali informacje dotyczące prawa do przenoszenia danych, zanim osoby, których dane dotyczą, zamkną jakiekolwiek konto, które posiadają. Umożliwia to użytkownikom przeanalizowanie swoich danych osobowych oraz ich łatwe przesłanie na własne urządzenie lub przesłanie innemu dostawcy przed rozwiązaniem umowy

Ponadto jako wiodącą praktykę do stosowania przez „otrzymujących" administratorów danych Grupa Robocza Art. 29 zaleca, aby zapewniali oni osobom, których dane dotyczą, kompletne informacje na temat charakteru danych osobowych, które są istotne dla świadczenia zapewnianych przez nich usług. Oprócz wspierania rzetelnego przetwarzania danych pozwala to użytkownikom ograniczyć zagrożenia dla osób trzecich, jak również ograniczyć wszelkie innego rodzaju niepotrzebne powielanie danych osobowych, nawet w przypadku braku zaangażowania jakichkolwiek innych osób, których dane dotyczą.

[24] Zgodnie z art. 12 administratorzy danych są zobowiązani do przekazywania „wszelkich informacji […] w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem – w szczególności gdy informacje są kierowane do dziecka".

- **W jaki sposób administrator danych może zidentyfikować osobę, której dane dotyczą, przed udzieleniem odpowiedzi na jej żądanie?**

W RODO nie ustanowiono żadnych bezwzględnie obowiązujących wymogów w zakresie sposobu uwierzytelniania osoby, której dane dotyczą. Art. 12 ust. 2 RODO stanowi jednak, że administrator danych nie odmawia podjęcia działań na żądanie osoby, której dane dotyczą, pragnącej wykonać przysługujące jej prawa (w tym prawo do przenoszenia danych), chyba że przetwarza dane osobowe w celu, który nie wymaga identyfikacji osoby, której dane dotyczą, oraz może on wykazać, iż nie jest w stanie zidentyfikować osoby, której dane dotyczą. Zgodnie z art. 11 ust. 2 w takich okolicznościach osoba, której dane dotyczą, może jednak dostarczyć dodatkowe informacje pozwalające ją zidentyfikować. Ponadto art. 12 ust. 6 stanowi, że jeżeli administrator danych ma uzasadnione wątpliwości odnośnie do tożsamości osoby, której dane dotyczą, może zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą. Jeżeli osoba, której dane dotyczą, dostarczy dodatkowe informacje pozwalające ją zidentyfikować, administrator danych nie odmawia podjęcia działań na żądanie tej osoby. Jeżeli informacje i dane gromadzone *online* są powiązane z pseudonimami lub unikatowymi identyfikatorami, administratorzy danych mogą wdrożyć odpowiednie procedury umożliwiające osobie fizycznej wniesienie żądania przeniesienia danych i otrzymanie odnoszących się do niej danych. W każdym razie administratorzy danych muszą wdrożyć procedurę uwierzytelniania, aby uzyskać całkowitą pewność odnośnie do tożsamości osoby, której dane dotyczą i która żąda swoich danych osobowych lub w ogólniejszym ujęciu wykonuje przysługujące jej prawa przyznane na mocy RODO.

Procedury te w wielu przypadkach już istnieją. Osoby, których dane dotyczą, często zostają już uwierzytelnione przez administratora danych przed zawarciem umowy lub uzyskaniem ich zgody na przetwarzanie. W rezultacie dane osobowe wykorzystywane do rejestracji osoby fizycznej, której dotyczy przetwarzanie, można również wykorzystać jako dowód uwierzytelnienia osoby, której dane dotyczą, do celów przeniesienia[25].

Chociaż w tych przypadkach uprzednia identyfikacja osób, których dane dotyczą, może wymagać żądania przedstawienia dowodu potwierdzającego ich tożsamość prawną, tego rodzaju weryfikacja może nie być właściwa do oceny powiązania między danymi a osobą fizyczną, której sprawa dotyczy, ponieważ takie powiązanie nie jest związane z tożsamością urzędową lub prawną. Co do zasady możliwość żądania przez administratora danych dostarczenia dodatkowych informacji w celu oceny tożsamości danej osoby nie może prowadzić do nadmiernych żądań oraz do gromadzenia danych osobowych, które nie są istotne lub niezbędne do wzmocnienia powiązania między tą osobą fizyczną a danymi osobowymi objętymi żądaniem.

Takie procedury uwierzytelniania istnieją już w wielu przypadkach. Przykładowo nazwy użytkownika i hasła są często wykorzystywane, aby umożliwić osobom fizycznym uzyskanie dostępu do danych zawartych na posiadanych przez nie kontach e-mail, kontach na portalach społecznościowych oraz kontach wykorzystywanych w ramach różnych innych usług, a w niektórych przypadkach osoby fizyczne zdecydowały się na korzystanie z niektórych spośród nich bez ujawniania swojego imienia i nazwiska oraz swojej tożsamości.

[25] Przykładowo, jeżeli przetwarzanie danych jest związane z kontem użytkownika, dostarczenie odpowiedniego loginu i hasła może być wystarczające do identyfikacji osoby, której dane dotyczą.

Jeżeli rozmiar danych żądanych przez osobę, której dane dotyczą, powoduje, że ich przesłanie za pośrednictwem internetu może być problematyczne, zamiast potencjalnego skorzystania z możliwości przedłużenia terminu na spełnienie żądania o maksymalnie trzy miesiące[26] administrator danych może również rozważyć alternatywne środki dostarczenia danych, takie jak transmisja strumieniowa lub zapisanie na płycie CD, DVD lub innym nośniku fizycznym, bądź zezwolenie na przesłanie danych osobowych bezpośrednio innemu administratorowi danych (zgodnie z art. 20 ust. 2 RODO, o ile jest to technicznie możliwe).

- **Jaki termin wyznaczono na udzielenie odpowiedzi na żądanie przeniesienia?**

Zgodnie z art. 12 ust. 3 administrator danych udziela „informacji o działaniach podjętych w związku z żądaniem" osobie, której dane dotyczą, „bez zbędnej zwłoki", a w każdym razie „w terminie miesiąca od otrzymania żądania". Wspomniany miesięczny termin można przedłużyć o kolejne trzy miesiące z uwagi na skomplikowany charakter sprawy, pod warunkiem że osobę, której dane dotyczą, poinformowano o przyczynach takiego opóźnienia w terminie miesiąca od dnia wniesienia pierwotnego żądania.

Istnieje prawdopodobieństwo, że administratorzy danych świadczący usługi społeczeństwa informacyjnego będą lepiej przygotowani do spełniania żądań w bardzo krótkim terminie. Aby sprostać oczekiwaniom użytkownika, dobrą praktyką jest określenie terminu, w jakim co do zasady można uzyskać odpowiedź na żądanie przeniesienia danych, oraz powiadomienie o nim osób, których dane dotyczą.

Administratorzy danych, którzy odmawiają udzielenia odpowiedzi na żądanie przeniesienia zgodnie z art. 12 ust. 4, informują osobę, której dane dotyczą, „o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem" najpóźniej w terminie miesiąca od otrzymania żądania.

Administratorzy danych muszą przestrzegać obowiązku udzielenia odpowiedzi w wyznaczonych terminach, nawet jeżeli jest to odpowiedź odmowna. Innymi słowy, administrator danych nie może zachować milczenia w przypadku zwrócenia się do niego o udzielenie odpowiedzi na żądanie przeniesienia danych.

- **W jakich przypadkach można odrzucić żądanie przeniesienia danych lub pobrać opłatę?**

W art. 12 administratorom danych zakazuje się pobierania opłaty za przekazanie danych osobowych, chyba że administrator danych może wykazać, że żądania są ewidentnie nieuzasadnione lub nadmierne, „w szczególności ze względu na swój ustawiczny charakter". W przypadku usług społeczeństwa informacyjnego, które specjalizują się w zautomatyzowanym przetwarzaniu danych osobowych, wdrożenie zautomatyzowanych systemów, takich jak interfejs programowania aplikacyjnego[27], może ułatwić wymianę z osobą, której dane dotyczą, a zatem zmniejszyć potencjalne obciążenie wynikające z ustawicznych żądań. Powinno być zatem bardzo niewiele przypadków, w których

[26] Art. 12 ust. 3: „Administrator [...] udziela [...] informacji o działaniach podjętych w związku z żądaniem".
[27] Interfejs programowania aplikacyjnego oznacza interfejsy aplikacji lub usług sieciowych udostępniane przez administratorów danych w taki sposób, aby inne systemy lub aplikacje mogły łączyć się i pracować z ich systemami.

administrator danych byłby w stanie uzasadnić odmowę dostarczenia informacji objętych żądaniem, nawet w odniesieniu do wielokrotnych żądań przeniesienia danych.

Ponadto przy określaniu nadmiernego charakteru żądania nie należy brać pod uwagę całkowitego kosztu procedur ustanowionych w celu udzielania odpowiedzi na żądania przeniesienia danych. W istocie w art. 12 RODO skoncentrowano się na żądaniach wnoszonych przez jedną osobę, której dane dotyczą, a nie na łącznej liczbie żądań otrzymanych przez administratora danych. W związku z tym całkowitymi kosztami wdrożenia systemu nie można obciążać osób, których dane dotyczą, ani nie można wykorzystywać tego rodzaju kosztów jako uzasadnienia odmowy udzielenia odpowiedzi na żądania przeniesienia.

V. W jaki sposób należy przekazywać dane podlegające przenoszeniu?

- **Jakie są oczekiwane środki, które powinien wdrożyć administrator danych w celu przekazania danych?**

Art. 20 ust. 1 RODO stanowi, że osoby, których dane dotyczą, mają prawo przesłać dane innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe.

Tego rodzaju przeszkody można określić jako bariery prawne, techniczne lub finansowe ustanowione przez administratora danych w celu powstrzymania lub spowolnienia dostępu, przesyłania lub ponownego wykorzystania przez osobę, której dane dotyczą, lub przez innego administratora danych. Przykładowo taką przeszkodę mogą stanowić: żądanie wniesienia opłaty z tytułu przekazania danych, brak interoperacyjności lub dostępu do formatu danych, interfejsu programowania aplikacyjnego lub dostarczonego formatu, nadmierna zwłoka lub złożoność w odniesieniu do uzyskania pełnego zbioru danych, celowe zamaskowanie zbioru danych lub szczególne i nieuzasadnione lub nadmierne żądania sektorowej normalizacji lub akredytacji[28].

Ponadto w art. 20 ust. 2 nałożono na administratorów danych obowiązki przesłania danych podlegających przenoszeniu bezpośrednio innym administratorom danych, „o ile jest to technicznie możliwe".

Techniczną możliwość przesłania danych przez administratora danych innemu administratorowi danych pod kontrolą osoby, której dane dotyczą, należy oceniać w poszczególnych przypadkach. W motywie 68 dokładniej wyjaśniono granice określenia „technicznie możliwe", wskazując, że omawiane prawo „nie powinno nakładać na administratorów obowiązku prowadzenia lub wprowadzenia kompatybilnych technicznie systemów przetwarzania".

Od administratorów danych oczekuje się przesyłania danych osobowych w interoperacyjnym formacie, chociaż nie nakłada to obowiązku obsługi tych formatów na innych administratorów danych. Bezpośrednie przesłanie danych przez jednego administratora danych innemu administratorowi mogłoby mieć zatem miejsce wówczas, gdy możliwa jest

[28] Mogą wystąpić określone przeszkody prawne, takie jak przeszkody związane z prawami i wolnościami innych wskazane w art. 20 ust. 4 lub przeszkody związane z bezpieczeństwem własnych systemów administratorów. Uzasadnienie, dlaczego takie przeszkody byłyby zgodne z prawem oraz dlaczego nie stanowią one przeszkody w rozumieniu art. 20 ust. 1, należy do obowiązków administratora danych.

komunikacja między dwoma systemami w zabezpieczony sposób[29] oraz gdy system otrzymujący ma techniczną możliwość odebrania przychodzących danych. Jeżeli przeszkody techniczne uniemożliwiają bezpośrednie przesłanie, administrator danych wyjaśnia istotę tych przeszkód osobom, których dane dotyczą, ponieważ w przeciwnym razie jego decyzja wywoła skutek podobny do odmowy podjęcia działań w związku z żądaniem osoby, której dane dotyczą (art. 12 ust. 4).

Na poziomie technicznym administratorzy danych powinni zbadać i ocenić dwa różne i uzupełniające się sposoby udostępniania danych podlegających przenoszeniu osobom, których dane dotyczą, lub innym administratorom danych:

- bezpośrednie przesłanie całego zbioru danych zawierającego dane podlegające przenoszeniu (lub kilku fragmentów części globalnego zbioru danych);
- zautomatyzowane narzędzie umożliwiające wyodrębnianie istotnych danych.

Drugi sposób może być preferowany przez administratorów danych w przypadkach obejmujących złożone, obszerne zbiory danych, ponieważ umożliwia on wyodrębnienie jakiejkolwiek części zbioru danych, która jest istotna dla osoby, której dane dotyczą, w kontekście jej żądania, może pomóc zminimalizować ryzyko oraz potencjalnie umożliwia wykorzystanie mechanizmów synchronizacji danych[30] (np. w kontekście regularnej komunikacji między administratorami danych). Może być to lepszy sposób zapewnienia zgodności w przypadku „nowego" administratora oraz stanowiłby on dobrą praktykę w zakresie ograniczania zagrożeń dla prywatności ze strony pierwotnego administratora danych.

Powyższe dwa różne i potencjalnie uzupełniające się sposoby przekazywania istotnych danych podlegających przenoszeniu można wdrożyć, udostępniając dane za pośrednictwem różnych środków, takich jak np. zabezpieczona wymiana komunikatów, serwer SFTP, interfejs programowania aplikacyjnego sieci Web lub portal sieci Web. Osoby, których dane dotyczą, powinny mieć możliwość korzystania z usług przechowywania danych osobowych, z systemu zarządzania danymi osobowymi[31] lub z innych rodzajów usług świadczonych przez zaufane osoby trzecie w celu przechowywania danych osobowych i udzielania administratorom danych pozwolenia na dostęp do danych i na ich przetwarzanie według potrzeb.

- **Jaki jest oczekiwany format danych?**

W RODO nałożono na administratorów danych wymogi przekazywania danych osobowych żądanych przez osobę fizyczną w formacie umożliwiającym ich ponowne wykorzystanie. W szczególności art. 20 ust. 1 RODO stanowi, że dane osobowe należy przekazać „w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu

[29] Za pośrednictwem uwierzytelnionej komunikacji o niezbędnym poziomie szyfrowania danych.
[30] Mechanizm synchronizacji może pomóc w wykonaniu ogólnych obowiązków przewidzianych w art. 5 RODO, który stanowi, że „dane osobowe muszą być [...] prawidłowe i w razie potrzeby uaktualniane".
[31] W odniesieniu do systemów zarządzania danymi osobowymi (PIMS) zob. na przykład opinia EIOD 9/2016 dostępna pod adresem https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-10-20_PIMS_opinion_EN.pdf

maszynowego". W motywie 68 przedstawiono dodatkowe wyjaśnienie, zgodnie z którym format ten powinien być interoperacyjny, przy czym termin ten definiuje się[32] w UE jako:

> „możliwość współdziałania różnych odrębnych organizacji na rzecz osiągnięcia uzgodnionych i korzystnych dla wszystkich stron celów, przy jednoczesnym dzieleniu się informacjami i wiedzą pomiędzy tymi organizacjami poprzez wspierane przez nie procesy biznesowe, za pomocą wymiany danych za pośrednictwem odpowiednich systemów TIK".

Terminy „ustrukturyzowany", „powszechnie używany" i „nadający się do odczytu maszynowego" stanowią zestaw minimalnych wymogów, które powinny umożliwiać interoperacyjność formatu danych przekazanych przez administratora danych. W ten sposób terminy „ustrukturyzowany, powszechnie używany i nadający się do odczytu maszynowego" stanowią określenia środków, natomiast interoperacyjność stanowi pożądany wynik.

W motywie 21 dyrektywy 2013/37/UE[33][34] zdefiniowano termin „przeznaczony do odczytu komputerowego" jako:

> „format pliku zorganizowany tak, aby aplikacje komputerowe mogły łatwo zidentyfikować, rozpoznać i uzyskać określone dane, w tym poszczególne stwierdzenia faktów, i ich wewnętrzną strukturę. Dane zakodowane w plikach zorganizowanych w formacie przeznaczonym do odczytu komputerowego to dane przeznaczone do odczytu komputerowego. Formaty przeznaczone do odczytu komputerowego mogą być otwarte lub zastrzeżone; mogą one występować jako standardy formalne lub nie. Dokumentów zakodowanych w formacie pliku ograniczających przetwarzanie automatyczne z powodu niemożności pozyskania danych lub utrudnień w ich pozyskaniu z tych dokumentów nie należy uznawać za sporządzone w formacie przeznaczonym do odczytu komputerowego. Państwa członkowskie powinny w stosownych przypadkach zachęcać do korzystania z formatów otwartych przeznaczonych do odczytu komputerowego".

Biorąc pod uwagę szeroki zakres potencjalnych rodzajów danych, które administrator danych może przetworzyć, w RODO nie przedstawiono szczegółowych zaleceń odnośnie do formatu przekazywanych danych osobowych. Najodpowiedniejszy format będzie zależał od sektora – odpowiednie formaty mogą już istnieć i zawsze należy je wybierać, dążąc do celu, jakim jest możliwość ich interpretacji i zapewnienie osobie, której dane dotyczą, znacznych możliwości przenoszenia danych. Formaty podlegające kosztownym ograniczeniom w zakresie udzielania licencji nie zostałyby jako takie uznane za właściwe podejście.

W motywie 68 wyjaśniono, że „przysługujące osobie, której dane dotyczą, prawo do przesłania lub otrzymania swoich danych osobowych nie powinno nakładać na administratorów obowiązku prowadzenia lub wprowadzenia kompatybilnych technicznie systemów przetwarzania". **Celem przenoszenia jest zatem interoperacyjność systemów, a nie ich kompatybilność**[35].

Oczekuje się, że dane osobowe będą przekazywane w formatach o wysokim poziomie abstrakcji względem wszelkich formatów wewnętrznych lub zastrzeżonych. Przenoszenie danych oznacza zatem dodatkową warstwę przetwarzania danych przez administratorów danych w celu uzyskania danych z platformy i wyodrębnienia danych osobowych nieobjętych zakresem przenoszenia danych, takich jak dane wywnioskowane lub dane związane z bezpieczeństwem systemów. W ten sposób administratorów danych zachęca się do wcześniejszego zidentyfikowania danych objętych zakresem przenoszenia we własnych systemach. Tego rodzaju dodatkowe przetwarzanie danych będzie uznawane za pomocnicze w stosunku do głównego przetwarzania danych, ponieważ nie dokonuje się go, aby osiągnąć nowy cel określony przez administratora danych.

Jeżeli żadne formaty nie są powszechnie używane w danej branży lub w określonym kontekście, **administratorzy danych powinni przekazać dane osobowe w powszechnie używanych formatach otwartych (np. XML, JSON, CSV itd.) wraz z** przydatnymi **metadanymi o najwyższym możliwym poziomie szczegółowości** przy jednoczesnym zachowaniu wysokiego poziomu abstrakcji. Odpowiednie metadane należy jako takie wykorzystywać w celu prawidłowego opisania znaczenia informacji będących przedmiotem wymiany. Takie metadane powinny być wystarczające dla umożliwienia funkcjonowania i ponownego wykorzystywania danych, jednak oczywiście bez ujawniania tajemnic handlowych. Jest zatem mało prawdopodobne, by przekazanie osobie fizycznej wersji skrzynki odbiorczej e-mail w formacie PDF miało wystarczająco ustrukturyzowany lub opisowy charakter dla umożliwienia łatwego ponownego wykorzystania danych dotyczących skrzynki odbiorczej. Dane dotyczące wiadomości e-mail należy przekazywać w formacie zachowującym wszystkie metadane, aby umożliwić skuteczne ponowne wykorzystanie danych. W takiej sytuacji podczas wyboru formatu danych, w jakim dane osobowe mają zostać przekazane, administrator danych powinien uwzględnić sposób, w jaki format ten może wpłynąć na prawo danej osoby fizycznej do ponownego wykorzystania danych lub w jaki może on to prawo ograniczyć. W przypadkach, w których administrator danych może zapewnić osobie, której dane dotyczą, możliwość wyboru preferowanego formatu danych osobowych, należy udzielić tej osobie zrozumiałego wyjaśnienia skutków, jakie wywoła określony wybór. Przetwarzanie dodatkowych metadanych wyłącznie dlatego, że mogłyby one być potrzebne lub pożądane w celu udzielenia odpowiedzi na żądanie przeniesienia danych, nie zapewnia jednak podstawy prawnej takiego przetwarzania.

Grupa Robocza Art. 29 usilnie zachęca zainteresowane strony w branży i stowarzyszenia branżowe do wspólpracy i opracowania wspólnego zbioru standardów i formatów interoperacyjnych, aby spełnić wymogi dotyczące prawa do przenoszenia danych. Jednym z instrumentów stworzonych w celu stawienia czoła temu wyzwaniu są europejskie ramy interoperacyjności, które przyczyniły się do wypracowania uzgodnionego podejścia do interoperacyjności w odniesieniu do organizacji, które pragną wspólnie świadczyć usługi publiczne. W ramach tych – w zakresie ich stosowania – określono zestaw

[32] Art. 2 decyzji Parlamentu Europejskiego i Rady nr 922/2009/WE z dnia 16 września 2009 r. w sprawie rozwiązań interoperacyjnych dla europejskich administracji publicznych (ISA), Dz.U. L 260 z 3.10.2009, s. 20.
[33] Zmieniająca dyrektywę 2003/98/WE w sprawie ponownego wykorzystywania informacji sektora publicznego.
[34] Glosariusz UE (http://eur-lex.europa.eu/eli-register/glossary.html) zawiera dalsze wyjaśnienie dotyczące oczekiwań związanych z pojęciami stosowanymi w niniejszych wytycznych, takich jak „nadający się do odczytu maszynowego", „interoperacyjność", „format otwarty", „standard", „metadane".

[35] W ISO/IEC 2382-01 zdefiniowano interoperacyjność w następujący sposób: „zdolność różnych elementów funkcjonalnych systemów informatycznych do komunikacji, uruchamiania programów lub przesyłania danych pomiędzy nimi w sposób niewymagający od ich od użytkownika żadnej wiedzy lub wymagający od niego wiedzy minimalnej na temat unikalnych właściwości tych elementów".

wspólnych elementów, takich jak słownictwo, pojęcia, zasady, polityki, wytyczne, zalecenia, normy, specyfikacje i praktyki[36].

- **W jaki sposób należy postępować w przypadku zbierania danych osobowych na szeroką skalę lub złożonego gromadzenia danych?**

W RODO nie wyjaśniono, w jaki sposób można zmierzyć się z wyzwaniem udzielenia odpowiedzi w przypadku zbierania danych na szeroką skalę, złożonej struktury danych lub wystąpienia innych problemów technicznych, które mogą przysparzać trudności administratorom danych lub osobom, których dane dotyczą.

We wszystkich jednak przypadkach kluczowe jest, aby dana osoba fizyczna była w stanie w pełni zrozumieć definicję, schemat i strukturę danych osobowych, które mogą zostać przekazane przez administratora danych. Przykładowo dane można w pierwszej kolejności przekazać w skróconej formie z wykorzystaniem pulpitów nawigacyjnych, umożliwiając osobie, której dane dotyczą, przenoszenie podzbiorów danych osobowych, a nie wszystkich danych. Administrator danych powinien przedstawić sens „w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem" (zob. art. 12 ust. 1 RODO) w taki sposób, aby osoba, której dane dotyczą, zawsze dysponowała jednoznacznymi informacjami na temat danych, jakie należy pobrać lub przesłać innemu administratorowi danych w związku z określonym celem. Przykładowo osoby, których dane dotyczą, powinny być w stanie korzystać z aplikacji oprogramowania w celu łatwego zidentyfikowania, rozpoznania lub przetwarzania określonych danych, które są tam zawarte.

Jak wskazano powyżej, praktycznym sposobem, w jaki administrator danych może udzielić odpowiedzi na żądania przeniesienia danych, jest zapewnienie odpowiednio zabezpieczonego i udokumentowanego interfejsu programowania aplikacyjnego. Może to umożliwić osobom fizycznym wnoszenie żądań dotyczących ich danych osobowych do administratora danych za pośrednictwem własnego oprogramowania lub oprogramowania osoby trzeciej bądź udzielenie pozwolenia innym podmiotom na wniesienie żądania w ich imieniu (w tym innemu administratorowi danych), jak określono w art. 20 ust. 2 RODO. Udzielając dostępu do danych za pośrednictwem zewnętrznie dostępnego interfejsu programowania aplikacyjnego, można również zapewnić bardziej skomplikowany system dostępu, który umożliwia osobom fizycznym wnoszenie kolejnych żądań dotyczących danych w formie pełnego pobrania albo w formie funkcji delta obejmującej wyłącznie zmiany, które zaszły od czasu ostatniego pobrania, przy czym tego rodzaju dodatkowe żądania nie mogą być uciążliwe dla administratora danych.

- **W jaki sposób można zabezpieczyć dane podlegające przenoszeniu?**

Co do zasady zgodnie z art. 5 ust. 1 lit. f) RODO administratorzy danych powinni zapewnić „odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych".

Przekazywanie danych osobowych osobie, której dane dotyczą, może jednak wiązać się również z pewnymi problemami pod względem bezpieczeństwa:

[36] Źródło: http://ec.europa.eu/isa/documents/isa_annex_ii_eif_en.pdf

W jaki sposób administratorzy danych mogą zapewnić bezpieczne przekazanie danych osobowych właściwej osobie?

Ponieważ przenoszenie danych ma na celu pozyskanie danych osobowych z systemu informacyjnego administratora danych, przesłanie może stać się potencjalnym źródłem zagrożenia dotyczącego tych danych (w szczególności naruszeń ochrony danych podczas przesyłania). Administrator danych odpowiada za podjęcie wszelkich środków bezpieczeństwa potrzebnych w celu zapewnienia nie tylko bezpiecznego przesłania danych osobowych (przy wykorzystaniu pełnego szyfrowania transmisji lub szyfrowania danych) do właściwego miejsca przeznaczenia (przy wykorzystaniu silnych środków uwierzytelniających), ale także dalszej ochrony danych osobowych, które pozostają w jego systemie, jak również przejrzystych procedur postępowania w przypadku możliwych naruszeń ochrony danych[37]. Administratorzy danych powinni zatem ocenić szczególne zagrożenia związane z przenoszeniem danych i podjąć właściwe środki zmniejszające ryzyko.

Tego rodzaju środki zmniejszające ryzyko mogłyby obejmować: jeżeli uwierzytelnienie osoby, której dane dotyczą, jest konieczne już w danym momencie – wykorzystanie dodatkowych informacji uwierzytelniających takich jak wspólna tajemnica lub innego składnika uwierzytelnienia takiego jak hasło jednorazowe; zawieszenie lub zamrożenie przesyłania w przypadku powzięcia podejrzenia włamania na konto; w przypadku bezpośredniego przesyłania danych osobowych przez jednego administratora danych innemu administratorowi należy zastosować uwierzytelnianie na podstawie upoważnienia, takie jak uwierzytelnianie za pośrednictwem tokena.

Tego rodzaju środki bezpieczeństwa nie mogą utrudniać ani uniemożliwiać użytkownikom wykonywania przysługujących im praw, np. poprzez nałożenie dodatkowych kosztów.

W jaki sposób można pomóc użytkownikom w zabezpieczeniu przechowywania danych osobowych w ich własnych systemach?

W przypadku pozyskiwania danych osobowych z usługi *online* zawsze istnieje ryzyko, że użytkownicy mogą przechowywać je w mniej zabezpieczonych systemach niż system zapewniany przez tę usługę. Osoba, której dane dotyczą, żądająca danych odpowiada za identyfikację właściwych środków w celu zabezpieczenia danych osobowych we własnym systemie. Należy ją jednak o tym poinformować, aby umożliwić jej podjęcie kroków w celu ochrony informacji, które otrzymała. Jako przykład dominującej praktyki administratorzy danych mogą również zalecić właściwy format (właściwe formaty), narzędzia szyfrowania i inne środki bezpieczeństwa, aby pomóc osobie, której dane dotyczą, w osiągnięciu tego celu.

* * *

Sporządzono w Brukseli dnia 13 grudnia 2016 r.

W imieniu Grupy Roboczej
Przewodnicząca

[37] Zgodnie z dyrektywą (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii.

Isabelle FALQUE-PIERROTIN

Ostatnio zmienione i przyjęte w dniu 5 kwietnia 2017 r.

W imieniu Grupy Roboczej
Przewodnicząca
Isabelle FALQUE-PIERROTIN

WP242 ZAŁĄCZNIK – Często zadawane pytania

1. **Czemu służy prawo do przenoszenia danych?**

Dzięki przenoszeniu danych osoby, których dane dotyczą, mają zasadniczo możliwość uzyskania i ponownego wykorzystania „swoich" danych do własnych celów i do skorzystania z różnych usług. To prawo ułatwia tym osobom przenoszenie, kopiowanie lub przekazywanie danych osobowych między środowiskami IT bez przeszkód. Oczekuje się, że – obok wzmocnienia pozycji konsumenta poprzez uniemożliwienie uzależnienia od jednego dostawcy – prawo to będzie sprzyjać innowacji i współdzieleniu danych osobowych między administratorami danych w sposób bezpieczny i pewny, pod kontrolą osoby, której dane dotyczą.

2. **Jakie możliwości daje korzystanie z prawa do przenoszenia danych?**

Po pierwsze, jest to prawo do **otrzymania danych osobowych** („w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego") przetwarzanych przez administratora danych i do przechowywania ich do dalszego użytku własnego na urządzeniu prywatnym bez przekazywania ich innemu administratorowi danych. To prawo oferuje osobom, których dane dotyczą, łatwy sposób osobistego zarządzania swoimi danymi osobowymi.
Po drugie, prawo to daje osobom, których dane dotyczą, możliwość przekazywania ich danych osobowych przez jednego administratora danych innemu administratorowi „bez przeszkód" oraz ułatwia tym osobom przenoszenie, kopiowanie lub przekazywanie danych osobowych między środowiskami IT.

3. **Jakie są narzędzia zalecane do udzielania odpowiedzi na żądania przeniesienia danych?**

Po pierwsze, administratorzy danych powinni zaoferować osobom, których dane dotyczą, możliwość bezpośredniego pobrania danych. Po drugie, powinni umożliwić osobom, których dane dotyczą, bezpośrednie przekazanie danych innemu administratorowi danych. Można to zrealizować np. poprzez udostępnienie interfejsu programowania aplikacyjnego.

Osoby, których dane dotyczą, mogą także korzystać z usług przechowywania danych osobowych przez zaufaną osobę trzecią, która przechowuje dane osobowe i udziela administratorom danych pozwolenia na dostęp do danych i na ich przetwarzanie według potrzeb, aby dane można było łatwo przekazywać między różnymi administratorami danych.

4. **W jakim stopniu administratorzy danych są odpowiedzialni za przekazywane lub otrzymywane dane w związku z korzystaniem z prawa do przenoszenia danych?**

Administratorzy danych, którzy udzielają odpowiedzi na żądania przeniesienia danych, nie odpowiadają za przetwarzanie danych przez osobę, której dane dotyczą, ani przez inne przedsiębiorstwo otrzymujące dane osobowe. Jednocześnie administrator otrzymujący dane odpowiada za zapewnienie, aby dane podlegające przeniesieniu były stosowne i nie były nadmierne w odniesieniu do nowego przetwarzania danych, aby odpowiednio poinformowano osobę, której dane dotyczą, o celu tego nowego przetwarzania, a także – w kontekście ogólnym – aby administratorzy przestrzegali zasad ochrony danych mających zastosowanie

do przetwarzania przez nich danych zgodnie z przepisami określonymi w ogólnym rozporządzeniu o ochronie danych (RODO).

5. Czy korzystanie z prawa do przenoszenia danych wpływa na korzystanie z pozostałych praw osób, których dane dotyczą?

Osoba fizyczna korzysta ze swojego prawa do przenoszenia danych (lub innego prawa określonego w RODO) bez uszczerbku dla jakichkolwiek innych praw. Osoba, której dane dotyczą, może korzystać ze swoich praw, o ile administrator danych nadal przetwarza dane. Na przykład osoba, której dane dotyczą, może w dalszym ciągu korzystać i czerpać korzyści z usług administratora danych nawet po przeprowadzeniu operacji przeniesienia danych. Podobnie, jeżeli osoba ta chce skorzystać z przysługującego jej prawa do usunięcia danych, sprzeciwienia się usunięciu lub uzyskania dostępu do swoich danych osobowych, administrator danych nie może wykorzystać poprzedniego lub kolejnego skorzystania z prawa do przenoszenia danych jako sposobu na opóźnienie lub odmowę odpowiedzi na inne prawa osoby, której dane dotyczą. Co więcej, przenoszenie danych nie powoduje automatycznego usunięcia danych z systemów administratora danych i nie wpływa na pierwotny okres przechowywania, który ma zastosowanie do przekazanych danych zgodnie z prawem do przenoszenia danych.

6. Kiedy ma zastosowanie prawo do przenoszenia danych?

To nowe prawo stosuje się, jeżeli spełnione są **3 łączne warunki**.
Po pierwsze, żądane dane osobowe należy przetworzyć w sposób zautomatyzowany (tj. z wyłączeniem nośników papierowych) na podstawie wcześniejszej zgody osoby, której dane dotyczą, lub na podstawie realizacji umowy, której stroną jest osoba, której dane dotyczą.

Po drugie, żądane dane osobowe powinny dotyczyć osoby, której dane dotyczą, a także powinny być dostarczone przez tę osobę. Grupa Robocza Art. 29 zaleca, aby administratorzy danych nie przyjmowali zbyt surowej interpretacji zdania „dane osobowe dotyczące osoby, której dane dotyczą", jeżeli dane osób trzecich znajdują się w zbiorze danych odnoszącym się do osoby, której dane dotyczą, i dostarczonych przez tę osobę oraz jeżeli osoba, której dane dotyczą i która występuje o te dane, wykorzystuje te dane do celów osobistych. Do typowych przykładów zbiorów danych zawierających dane osób trzecich należą zapisy rozmów telefonicznych (w tym rozmowy przychodzące i wychodzące), które osoba, której dane dotyczą, chciałaby otrzymać lub historia konta bankowego, która zawiera płatności przychodzące od osób trzecich.

Dane osobowe można uznać za dostarczone przez osobę, której dane dotyczą, jeżeli są one świadomie i czynnie „dostarczone" przez osobę, której dane dotyczą, jak ma to miejsce w przypadku danych konta (np. adresu e-mail, nazwy użytkownika, wieku) podawanych w formularzach online, ale również jeżeli są one generowane i gromadzone na podstawie działań użytkowników w ramach użytkowania usługi lub urządzenia. Z kolei dane osobowe, które pochodzą lub które można wywnioskować z danych dostarczonych przez osobę, której dane dotyczą, takie jak profil użytkownika stworzony w oparciu o analizę nieprzetworzonych inteligentnych pomiarów, nie mieszczą się w zakresie prawa do przenoszenia danych, ponieważ nie dostarcza ich osoba, której dane dotyczą, ale tworzą je administratorzy danych.

Zgodnie z trzecim warunkiem korzystanie z tego nowego prawa nie powinno wpływać niekorzystnie na prawa i wolności osób trzecich. Przykładowo, jeżeli w zbiorze danych przekazanym na żądanie osoby, której dane dotyczą, znajdują się dane osobowe związane z innymi osobami fizycznymi, nowy administrator danych powinien przetworzyć te dane wyłącznie wtedy, gdy istnieją ku temu odpowiednie podstawy prawne. Zazwyczaj odpowiednie będzie przetwarzanie danych pod wyłączną kontrolą osoby, której dane dotyczą, w ramach działalności czysto osobistej lub domowej.

7. W jaki sposób poinformować osoby, których dane dotyczą, o tym nowym prawie?

Administratorzy danych powinni przekazać osobom, których dane dotyczą, informacje o istnieniu prawa do przenoszenia danych „w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem". W tym zakresie Grupa Robocza Art. 29 zaleca, aby administratorzy danych jasno wyjaśnili różnicę między rodzajami danych, które osoba, której dane dotyczą, może otrzymać poprzez skorzystanie z prawa do przenoszenia lub z prawa do dostępu, a także aby przedstawili szczegółowe informacje na temat prawa do przenoszenia danych przed zamknięciem jakiegokolwiek konta, żeby osoby, których dane dotyczą, miały możliwość odzyskania i przechowywania swoich danych osobowych.
Ponadto administratorzy danych otrzymujący dane podlegające przeniesieniu na żądanie osoby, której dane dotyczą, mogą – w ramach najlepszej praktyki – zapewnić osobom, których dane dotyczą, kompletne informacje na temat charakteru danych osobowych istotnych dla wykonywania świadczonych przez nich usług.

8. W jaki sposób administrator danych może zidentyfikować osobę, której dane dotyczą, przed udzieleniem odpowiedzi na jej żądanie?

Grupa Robocza Art. 29 zaleca, aby administratorzy danych wprowadzili odpowiednie procedury umożliwiające osobie fizycznej złożenie żądania przeniesienia danych i otrzymanie związanych z nią danych. Administratorzy danych muszą korzystać z procedury weryfikacyjnej, aby upewnić się odnośnie do tożsamości osoby, której dane dotyczą i która składa wniosek o uzyskanie swoich danych osobowych lub, w ujęciu ogólnym, korzysta z praw przyznanych jej na mocy RODO.

9. Jaki termin wyznaczono na udzielenie odpowiedzi na żądanie przeniesienia?

W art. 12 administratorom danych zakazuje się pobierania opłaty za wydanie danych osobowych, chyba że administrator danych może wykazać, że żądania mają ewidentnie nieuzasadniony lub nadmierny charakter, „w szczególności ze względu na swój ustawiczny charakter". W przypadku usług społeczeństwa informacyjnego lub podobnych usług online, które specjalizują się w zautomatyzowanym przetwarzaniu danych osobowych, istnieje bardzo małe prawdopodobieństwo, że udzielanie odpowiedzi na wiele żądań o przeniesienie danych może stanowić nadmierne obciążenie. W tych przypadkach Grupa Robocza Art. 29 zaleca określenie zasadnych ram czasowych dostosowanych do kontekstu i poinformowanie o nich osób, których dane dotyczą.

10. W jaki sposób należy przekazywać dane podlegające przeniesieniu?

Dane osobowe należy przekazywać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego. Te specyfikacje mające zastosowanie do środków powinny gwarantować interoperacyjność formatu danych dostarczonych przez administratora danych, gdzie interoperacyjność oznacza pożądany wynik. Nie oznacza to jednak, że

administratorzy danych powinni utrzymywać kompatybilne systemy. Ponadto administratorzy danych powinni zapewnić jak najwięcej metadanych o najwyższym stopniu dokładności i szczegółowości, aby zachować dokładne znaczenie wymienionych informacji.

Biorąc pod uwagę szeroki zakres potencjalnych rodzajów danych, które administrator danych może przetworzyć, w RODO nie przedstawiono szczegółowych zaleceń odnośnie do formatu przekazywanych danych osobowych. Najodpowiedniejszy format będzie zależał od sektora – odpowiednie formaty mogą już istnieć i zawsze należy je wybierać, dążąc do celu, jakim jest możliwość ich interpretacji.

Grupa Robocza Art. 29 usilnie zachęca zainteresowane strony w branży i stowarzyszenia branżowe do współpracy i opracowania wspólnego zbioru standardów i formatów interoperacyjnych, aby spełnić wymogi dotyczące prawa do przenoszenia danych.

GRUPA ROBOCZA ART. 29

16/PL
WP 243 rev.01

Wytyczne dotyczące inspektorów ochrony danych („DPO")

Przyjęte w dniu 13 grudnia 2016 r.

Ostatnio zmienione i przyjęte w dniu 5 kwietnia 2017 r.

Grupa Robocza została powołana na mocy art. 29 dyrektywy 95/46/WE. Jest ona niezależnym europejskim organem doradczym w zakresie ochrony danych i prywatności. Zadania Grupy zostały określone w przepisach art. 30 dyrektywy 95/46/WE i art. 15 dyrektywy 2002/58/WE.

Obsługę sekretariatu zapewnia Dyrekcja C (prawa podstawowe i praworządność) Komisji Europejskiej, Dyrekcja Generalna ds. Sprawiedliwości i Konsumentów, B-1049 Bruksela, Belgia, biuro nr MO59 03/068.

Strona internetowa: http://ec.europa.eu/justice/data-protection/index_en.htm

GRUPA ROBOCZA DS. OCHRONY OSÓB FIZYCZNYCH W ZAKRESIE PRZETWARZANIA DANYCH OSOBOWYCH

powołana na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r.,

uwzględniając art. 29 i 30 tej dyrektywy,

uwzględniając swój regulamin wewnętrzny,

PRZYJMUJE NINIEJSZE WYTYCZNE:

Spis treści

1 WPROWADZENIE 5

2 WYZNACZANIE DPO 6

2.1. Obowiązkowe wyznaczenie 6

2.1.1 „Organ lub podmiot publiczny” 7
2.1.2 „Główna działalność” 8
2.1.3 „Na dużą skalę” 9
2.1.4 „Regularne i systematyczne monitorowanie” 10
2.1.5 Szczególne kategorie danych i dane dotyczące wyroków skazujących i naruszeń prawa 11

2.2. DPO podmiotu przetwarzającego 11

2.3. Wyznaczenie jednego DPO dla szeregu organizacji 12

2.4. Dostępność i lokalizacja DPO 13

2.5. Wiedza fachowa i umiejętności DPO 13

2.6. Publikowanie danych kontaktowych DPO i zawiadamianie o tych danych 15

3 STATUS DPO 15

3.1. Udział DPO we wszystkich sprawach dotyczących ochrony danych osobowych 15

3.2. Niezbędne zasoby 16

3.3. Instrukcje oraz „wykonywanie obowiązków i zadań w sposób niezależny” 17

3.4. Odwołanie lub kara za wypełnianie zadań DPO 18

3.5. Konflikt interesów 19

4 ZADANIA DPO 19

4.1. Monitorowanie przestrzegania RODO 19

4.2. Rola DPO w ramach oceny skutków dla ochrony danych 20

4.3. Współpraca z organem nadzorczym i pełnienie funkcji punktu kontaktowego 21

4.4. Podejście oparte na analizie ryzyka 21

4.5. Rola DPO w rejestrowaniu czynności przetwarzania 22

5 ZAŁĄCZNIK – WYTYCZNE DOTYCZĄCE DPO: CO TRZEBA WIEDZIEĆ? 23

WYZNACZENIE DPO 23

1 KTÓRE ORGANIZACJE SĄ ZOBOWIĄZANE WYZNACZYĆ DPO? 23

2 CO OZNACZA POJĘCIE „GŁÓWNA DZIAŁALNOŚĆ”? 23

3 CO OZNACZA POJĘCIE „NA DUŻĄ SKALĘ”? 24

4 CO OZNACZA POJĘCIE „REGULARNE I SYSTEMATYCZNE MONITOROWANIE”? 24

5 CZY ORGANIZACJE MOGĄ WSPÓLNIE WYZNACZYĆ DPO? JEŻELI TAK, TO NA JAKICH WARUNKACH? 25

6 GDZIE POWINNA ZNAJDOWAĆ SIĘ SIEDZIBA DPO? 25

7 CZY MOŻNA WYZNACZYĆ ZEWNĘTRZNEGO DPO? 26

8 JAKIE KWALIFIKACJE ZAWODOWE POWINIEN POSIADAĆ DPO?..... 26

STATUS DPO..... 27

9 JAKIE ZASOBY ADMINISTRATOR LUB PODMIOT PRZETWARZAJĄCY POWINNI ZAPEWNIĆ DPO?..... 27

10 JAKIE GWARANCJE NALEŻY USTANOWIĆ, ABY ZAPEWNIĆ DPO MOŻLIWOŚĆ SAMODZIELNEGO WYKONYWANIA POWIERZONYCH MU ZADAŃ? CO OZNACZA POJĘCIE „KONFLIKT INTERESÓW"?..... 27

ZADANIA DPO..... 28

11 CO OZNACZA TERMIN „MONITOROWANIE PRZESTRZEGANIA"?..... 28

12 CZY DPO PONOSI OSOBISTĄ ODPOWIEDZIALNOŚĆ ZA PRZYPADKI NARUSZENIA WYMOGÓW DOTYCZĄCYCH OCHRONY DANYCH?..... 28

13 JAKĄ ROLĘ PEŁNI DPO W PROCESIE OCENY SKUTKÓW DLA OCHRONY DANYCH I REJESTRU CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH?..... 28

1 Wprowadzenie

W ogólnym rozporządzeniu o ochronie danych („RODO")[1], które ma wejść w życie w dniu 25 maja 2018 r., przewidziano zmodernizowane ramy na rzecz przestrzegania przepisów w zakresie ochrony danych w Europie opierające się na zasadzie rozliczalności. W przypadku wielu organizacji kluczowym elementem tych nowych ram prawnych będą inspektorzy ochrony danych („DPO") odpowiedzialni za podejmowanie działań ułatwiających przestrzeganie przepisów RODO.

Przepisy RODO nakładają na niektórych administratorów i na niektóre podmioty przetwarzające obowiązek wyznaczenia DPO[2]. Obowiązek ten będzie spoczywał na wszystkich organach i podmiotach publicznych (niezależnie od rodzaju przetwarzanych przez nie danych), a także na innych organizacjach, które – w ramach swojej głównej działalności – zajmują się systematycznym monitorowaniem osób fizycznych na dużą skalę lub przetwarzają szczególne kategorie danych osobowych na dużą skalę.

Organizacje mogą niekiedy dobrowolnie wyznaczyć DPO nawet w przypadku, gdy w RODO nie ustanowiono wymogu wyznaczenia DPO. Grupa Robocza Art. 29 zachęca do podejmowania dobrowolnych wysiłków w tym obszarze.

Koncepcja DPO nie jest nową koncepcją. Choć w dyrektywie 95/46/WE[3] na żadną organizację nie nałożono wymogu wyznaczenia DPO, praktyka wyznaczania DPO wykształciła się mimo to na przestrzeni lat w szeregu państw członkowskich.

Przed przyjęciem RODO Grupa Robocza Art. 29 argumentowała, że DPO pełni kluczową rolę w procesie zapewniania rozliczalności oraz że wyznaczenie DPO może ułatwić przestrzeganie obowiązujących przepisów, zapewniając tym samym przedsiębiorstwom przewagę konkurencyjną[4]. Poza ułatwianiem przestrzegania obowiązujących przepisów poprzez wdrażanie narzędzi rozliczalności (np. usprawnianie procesu przeprowadzania ocen skutków dla ochrony danych i przeprowadzanie lub ułatwianie przeprowadzania audytów) DPO pełnią funkcję pośredników między

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), (Dz.U. L 119 z 4.5.2016). RODO ma znaczenie dla EOG i będzie miało zastosowanie po jego włączeniu do Porozumienia EOG.

[2] Właściwe organy są również zobowiązane do wyznaczenia DPO zgodnie z art. 32 dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylającej decyzję ramową Rady 2008/977/WSiSW (Dz.U. L 119 z 4.5.2016, s. 89–131) i zgodnie z krajowymi przepisami implementacyjnymi. Choć niniejsze wytyczne koncentrują się na DPO, o których mowa w RODO, mają również zastosowanie w odniesieniu do DPO, o których mowa w dyrektywie 2016/680, z uwagi na podobieństwo przepisów tych dwóch aktów prawnych.

[3] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.U. L 281 z 23.11.1995, s. 31).

[4] Zob. http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_appendix_core_issues_plenary_en.pdf

odpowiednimi zainteresowanymi stronami (np. organami nadzorczymi, osobami, których dane dotyczą, i oddziałami w ramach danej organizacji).

DPO nie ponosi osobistej odpowiedzialności za przypadki naruszenia przepisów RODO. RODO wyraźnie stanowi, że obowiązek zagwarantowania i wykazania, iż przetwarzanie danych odbywa się zgodnie z jego przepisami, spoczywa na administratorze lub podmiocie przetwarzającym (art. 24 ust. 1). Obowiązek zapewnienia zgodności środków w zakresie ochrony danych z przepisami rozporządzenia spoczywa na administratorze lub podmiocie przetwarzającym.

Administrator lub podmiot przetwarzający odgrywają również kluczową rolę w zapewnianiu DPO możliwości skutecznego wywiązywania się z powierzonych mu zadań. Wyznaczenie DPO to zaledwie pierwszy krok, ponieważ DPO należy również zapewnić wystarczający stopień autonomii i wystarczające zasoby, aby mógł on skutecznie wywiązywać się z powierzonych mu zadań.

W RODO uznano kluczową rolę DPO w nowym systemie zarządzania danymi i ustanowiono warunki dotyczące sposobu jego wyznaczania, jego statusu oraz spoczywających na nim obowiązków. Celem niniejszych wytycznych jest wyjaśnienie odpowiednich przepisów RODO, nie tylko aby ułatwić administratorom i podmiotom przetwarzającym przestrzeganie obowiązujących przepisów, ale również aby zapewnić DPO wsparcie w wywiązywaniu się z powierzonych im obowiązków. W wytycznych przedstawiono również zalecenia dotyczące najlepszych praktyk, które opracowano w oparciu o doświadczenia zgromadzone w niektórych państwach członkowskich UE. Grupa Robocza Art. 29 będzie monitorowała wdrażanie niniejszych wytycznych i może w stosownych przypadkach uzupełnić je o dodatkowe informacje.

2 Wyznaczanie DPO

2.1. Obowiązkowe wyznaczenie

Zgodnie z art. 37 ust. 1 RODO DPO należy wyznaczyć w trzech konkretnych przypadkach[5]:

a) jeżeli przetwarzania dokonują organ lub podmiot publiczny[6];
b) jeżeli główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę; lub
c) jeżeli główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych[7] albo[8] danych osobowych dotyczących wyroków skazujących i naruszeń prawa[9].

[5] Należy zwrócić uwagę na fakt, że art. 37 ust. 4 i przepisy obowiązujące w Unii lub w państwach członkowskich mogą wymagać wyznaczenia DPO również w innych sytuacjach.
[6] Z wyjątkiem sądów w ramach sprawowania przez nie wymiaru sprawiedliwości. Zob. art. 32 dyrektywy (UE) 2016/680.
[7] Zgodnie z art. 9 obejmuje to przetwarzanie danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzanie danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby.
[8] W art. 37 ust. 1 lit. c) użyto sformułowania „oraz". Aby uzyskać dodatkowe informacje na temat przyczyn, dla których zdecydowano się zastosować słowo „albo" zamiast słowa „oraz", zob. sekcja 2.1.5.
[9] Art. 10.

W poniższych podsekcjach Grupa Robocza Art. 29 przedstawiła wytyczne dotyczące kryteriów i terminologii zastosowanych w art. 37 ust. 1.

Grupa Robocza Art. 29 zaleca, aby – poza przypadkami, w których dana organizacja z oczywistych względów nie jest zobowiązana wyznaczyć DPO – administratorzy i podmioty przetwarzające dokumentowali przebieg prowadzonej przez siebie analizy wewnętrznej w celu ustalenia, czy w danym przypadku należy wyznaczyć DPO, aby mogli wykazać, że należycie uwzględnili stosowne czynniki[10]. Wspomniana analiza stanowi jeden z elementów procesu dokumentowania zgodnie z zasadą rozliczalności. Organ nadzorczy może zażądać przeprowadzenia tej analizy; ponadto – w stosownych przypadkach – należy ją aktualizować, np. w sytuacji, gdy administratorzy lub podmioty przetwarzające rozpoczną prowadzenie nowego rodzaju działalności lub świadczenie nowych usług, które mogą spełniać kryteria ustanowione w art. 37 ust. 1.

Jeżeli organizacja wyznaczyła DPO na zasadzie dobrowolności, wymogi przewidziane w art. 37–39 będą regulowały kwestie związane z wyznaczeniem takiego DPO, jego statusem i spoczywającymi na nim obowiązkami, tak jak gdyby został on wyznaczony w ramach obowiązku wyznaczenia DPO.

Nic nie stoi na przeszkodzie, aby organizacja, która zgodnie z obowiązującymi przepisami nie jest zobowiązana do wyznaczenia DPO i która nie chce wyznaczyć DPO na zasadzie dobrowolności, zatrudniła pracowników lub konsultantów zewnętrznych i powierzyła im zadania w obszarze ochrony danych osobowych. W takim przypadku należy zadbać o to, by nazwa stanowiska piastowanego przez daną osobę, jej pozycja i zakres powierzonych jej obowiązków nie wzbudzały żadnych wątpliwości. Dlatego też we wszelkich komunikatach publikowanych w ramach przedsiębiorstwa, a także we wszelkich komunikatach adresowanych do organów ochrony danych, osób, których dane dotyczą, i ogólnie rozumianej opinii publicznej, należy jednoznacznie wskazać, że taki pracownik lub konsultant nie pełni funkcji inspektora ochrony danych (DPO)[11].

DPO – niezależnie od tego, czy jego wyznaczenie było obowiązkowe, czy też został on wyznaczony na zasadzie dobrowolności – jest odpowiedzialny za wszystkie operacje przetwarzania prowadzone przez danego administratora lub przez dany podmiot przetwarzający.

2.1.1 „ORGAN LUB PODMIOT PUBLICZNY"

W RODO nie zawarto definicji pojęcia „organ lub podmiot publiczny". W opinii Grupy Roboczej Art. 29 pojęcie to powinno zostać zdefiniowane w ustawodawstwie krajowym. Za organy i podmioty publiczne uznaje się zatem organy na szczeblu krajowym, regionalnym i lokalnym, ale zgodnie z obowiązującymi przepisami krajowymi pojęcie to obejmuje również zazwyczaj szereg innych podmiotów podlegających przepisom prawa publicznego[12]. W takich przypadkach wyznaczenie DPO jest obowiązkowe.

Zadanie wykonywane w interesie publicznym może być realizowane, a władza publiczna może być sprawowana[13], nie tylko przez organy lub podmioty publiczne, ale również przez inne osoby fizyczne lub prawne podlegające przepisom prawa publicznego lub prywatnego w sektorach takich jak –

[10] Zob. art. 24 ust. 1.
[11] Dotyczy to również głównych urzędników ds. prywatności lub innych osób zawodowo zajmujących się kwestiami związanymi z prywatnością, którzy pracują już w niektórych przedsiębiorstwach i którzy mogą nie spełniać kryteriów ustanowionych w RODO, np. jeżeli chodzi o ilość dostępnych zasobów lub gwarancje niezależności – w takim przypadku nie można uznać ich za DPO ani określać ich tym mianem.

zgodnie z przepisami krajowymi obowiązującymi w poszczególnych państwach członkowskich – sektor usług transportu publicznego, sektor zaopatrzenia w wodę i energię, sektor infrastruktury drogowej, sektor publicznej działalności nadawczej, sektor mieszkalnictwa publicznego lub sektor organów dyscyplinarnych sprawujących nadzór nad prawidłowością wykonywania zawodów regulowanych.

W takich przypadkach osoby, których dane dotyczą, mogą znaleźć się w sytuacji bardzo podobnej do sytuacji, w której dochodziłoby do przetwarzania dotyczących ich danych przez organy lub podmioty publiczne. W szczególności dane można przetwarzać w podobnych celach, a osoby fizyczne niejednokrotnie mają równie niewielki wpływ na to, czy i w jaki sposób ich dane będą przetwarzane, lub wręcz w ogóle nie mają na to wpływu, co z kolei może wiązać się z koniecznością zapewnienia dodatkowej ochrony poprzez wyznaczenie DPO.

Choć wyznaczenie DPO nie jest obowiązkowe w takich przypadkach, Grupa Robocza Art. 29 zaleca, aby organizacje prywatne realizujące zadania wykonywane w interesie publicznym lub sprawujące władzę publiczną wyznaczały DPO na zasadzie dobrej praktyki. Taki DPO jest odpowiedzialny za wszystkie operacje przetwarzania, uwzględniając również operacje, które nie są związane z realizacją zadania wykonywanego w interesie publicznym ani z pełnieniem obowiązków urzędowych (np. zarządzanie bazą danych pracowników).

2.1.2 „GŁÓWNA DZIAŁALNOŚĆ"

W art. 37 ust. 1 lit. b) i c) RODO wspomina się o „głównej działalności administratora lub podmiotu przetwarzającego". W motywie 97 doprecyzowano, że „przetwarzanie danych osobowych jest główną działalnością administratora, jeżeli oznacza jego zasadnicze, a nie poboczne czynności". „Główna działalność" oznacza kluczowe operacje, które administrator lub podmiot przetwarzający muszą podjąć, aby osiągnąć swoje cele.

Pojęcie „główna działalność" nie powinno jednak być interpretowane jako wykluczające czynności, w przypadku których przetwarzanie danych stanowi nieodłączny element działalności prowadzonej przez administratora lub podmiot przetwarzający. Na przykład główną działalnością szpitala jest świadczenie usług w zakresie opieki zdrowotnej. Szpital nie mógłby jednak świadczyć tych usług w bezpieczny i skuteczny sposób, gdyby nie przetwarzał danych dotyczących zdrowia, takich jak dokumentacja medyczna pacjentów. Z tego względu przetwarzanie takich danych powinno zostać uznane za jeden z elementów głównej działalności każdego szpitala, co oznacza, że szpitale są zobowiązane wyznaczyć DPO.

Inny przykład, jaki można przywołać w tym miejscu, dotyczy prywatnej firmy ochroniarskiej zajmującej się sprawowaniem nadzoru nad szeregiem prywatnych centrów handlowych i obiektów publicznych. Sprawowanie nadzoru stanowi główną działalność tego przedsiębiorstwa, której wykonywanie nieodłącznie wiąże się z koniecznością przetwarzania danych osobowych. Dlatego też również to przedsiębiorstwo musi wyznaczyć DPO.

[12] Zob. np. definicje terminów „organ sektora publicznego" i „podmiot prawa publicznego" zawarte w art. 2 pkt 1 i 2 dyrektywy 2003/98/WE Parlamentu Europejskiego i Rady z dnia 17 listopada 2003 r. w sprawie ponownego wykorzystywania informacji sektora publicznego (Dz.U. L 345 z 31.12.2003, s. 90).
[13] Art. 6 ust. 1 lit. e).

Wszystkie organizacje podejmują natomiast określonego rodzaju działania, na przykład przy wypłacaniu wynagrodzeń swoim pracownikom lub przy podejmowaniu standardowych czynności w zakresie wsparcia IT. Są to przykłady funkcji wspierających, które mają kluczowe znaczenie dla głównej działalności lub głównego obszaru zainteresowań danej organizacji. Choć działania w tym zakresie są niezbędne i kluczowe, zazwyczaj uznaje się je za działania pomocnicze, a nie za element głównej działalności.

2.1.3 „NA DUŻĄ SKALĘ"

Zgodnie z art. 37 ust. 1 lit. b) i c) obowiązek wyznaczenia DPO pojawia się w przypadku, gdy przetwarzanie danych osobowych ma odbywać się na dużą skalę. W RODO nie zawarto definicji pojęcia „przetwarzanie na dużą skalę", choć w motywie 91 przedstawiono pewne wskazówki w tym zakresie[14].

Przedstawienie precyzyjnych danych liczbowych dotyczących ilości przetwarzanych danych albo liczby zainteresowanych osób, które można byłoby zastosować we wszystkich sytuacjach, nie jest możliwe. Nie wyklucza to jednak możliwości wypracowania – w miarę upływu czasu – standardowej praktyki umożliwiającej bardziej precyzyjne lub w większym stopniu zorientowane ilościowo identyfikowanie elementów, które można uznać za świadczące o działaniu „na dużą skalę", w różnego rodzaju powszechnych czynnościach przetwarzania. Grupa Robocza Art. 29 również planuje wnieść wkład w działania w tym zakresie, udostępniając i publikując przykłady odpowiednich progów, po przekroczeniu których powstaje obowiązek wyznaczenia DPO.

W każdym razie Grupa Robocza Art. 29 zaleca, aby przy ustalaniu, czy przetwarzanie danych odbywa się na dużą skalę, wziąć pod uwagę w szczególności następujące czynniki:

- liczbę osób, których dane dotyczą – wyrażoną jako konkretna wartość albo jako odsetek populacji odniesienia;
- ilość danych lub zakres poszczególnych przetwarzanych pozycji danych;
- czas trwania lub trwałość czynności przetwarzania danych;
- zakres geograficzny czynności przetwarzania.

[14] Zgodnie z treścią tego motywu pojęcie to obejmowałoby w szczególności „operacje przetwarzania o dużej skali – które służą przetwarzaniu znacznej ilości danych osobowych na szczeblu regionalnym, krajowym lub ponadnarodowym i które mogą wpłynąć na dużą liczbę osób, których dane dotyczą, oraz które mogą powodować wysokie ryzyko". W motywie tym stwierdzono natomiast wprost, że „przetwarzanie danych osobowych nie powinno być uznawane za przetwarzanie na dużą skalę, jeżeli dotyczy danych osobowych pacjentów lub klientów i jest dokonywane przez pojedynczego lekarza, innego pracownika służby zdrowia lub prawnika". Należy zwrócić uwagę na fakt, że choć w motywie przedstawiono skrajne przykłady (tj. zestawiono przetwarzanie danych przez pojedynczego lekarza z przetwarzaniem danych na szczeblu całego państwa lub całej Europy), między tymi dwiema skrajnymi sytuacjami występuje wiele mniej jednoznacznych przypadków. Ponadto należy pamiętać, że przywołany motyw dotyczy ocen skutków dla ochrony danych. Oznacza to, że niektóre z wymienionych w nim elementów mogą być specyficzne dla tego kontekstu, dlatego też proces wyznaczania DPO niekoniecznie musi przebiegać w dokładnie taki sam sposób.

Przykłady przetwarzania na dużą skalę obejmują:

- przetwarzanie danych pacjentów przez szpital w ramach prowadzonej przez niego działalności;
- przetwarzanie danych o podróży osób fizycznych korzystających z miejskiego systemu transportu publicznego (np. śledzenie za pośrednictwem biletów elektronicznych);
- przetwarzanie danych określających położenie geograficzne klientów międzynarodowej sieci restauracji typu fast-food w czasie rzeczywistym do celów statystycznych przez podmiot przetwarzający specjalizujący się w świadczeniu tego typu usług;
- przetwarzanie danych klientów przez zakład ubezpieczeń lub bank w ramach prowadzonej przez te podmioty działalności gospodarczej;
- przetwarzanie danych osobowych przez wyszukiwarkę internetową na potrzeby reklamy behawioralnej;
- przetwarzanie danych (treść, przepływ danych, lokalizacja) przez dostawców usług telefonicznych lub internetowych.

Przykłady działań, które nie stanowią przetwarzania na dużą skalę:

- przetwarzanie danych pacjenta przez pojedynczego lekarza;
- przetwarzanie danych osobowych dotyczących wyroków skazujących i naruszeń prawa przez pojedynczego prawnika.

2.1.4 „Regularne i systematyczne monitorowanie"

Choć pojęcie regularnego i systematycznego monitorowania osób, których dane dotyczą, nie zostało zdefiniowane w RODO, w motywie 24 wspomniano o pojęciu „monitorowania zachowania osób, których dane dotyczą"[15], które w oczywisty sposób obejmuje wszystkie formy śledzenia i profilowania w internecie na potrzeby reklamy behawioralnej.

Pojęcie monitorowania nie ogranicza się jednak wyłącznie do aktywności prowadzonej w internecie, a zjawisko śledzenia w internecie należy traktować wyłącznie jako przykładową metodę monitorowania zachowania osób, których dane dotyczą[16].

Zgodnie z wykładnią dokonaną przez Grupę Roboczą Art. 29, aby dane działanie można było uznać za „regularne", musi ono posiadać przynajmniej jedną z następujących cech:

- być aktualnie w toku lub być podejmowane w regularnych odstępach czasu w danym okresie;
- być prowadzone cyklicznie lub powtarzać się w określonych momentach;
- być prowadzone stale lub okresowo.

[15] „Aby stwierdzić, czy czynność przetwarzania można uznać za »monitorowanie zachowania« osób, których dane dotyczą, należy ustalić, czy osoby fizyczne są obserwowane w internecie, w tym także czy później potencjalnie stosowane są techniki przetwarzania danych polegające na profilowaniu osoby fizycznej, w szczególności w celu podjęcia decyzji jej dotyczącej lub przeanalizowania lub prognozowania jej osobistych preferencji, zachowań i postaw".

[16] Należy zwrócić uwagę na fakt, że motyw 24 dotyczy transgranicznego stosowania RODO. Ponadto istnieje również różnica między brzmieniem terminu „monitorowanie ich zachowania" (art. 3 ust. 2 lit. b)) a brzmieniem terminu „regularne i systematyczne monitorowanie osób, których dane dotyczą" (art. 37 ust. 1 lit. b)), co może być postrzegane jako przesłanka świadcząca o tym, że wspomniane dwa terminy odnoszą się do różnych pojęć.

Zgodnie z wykładnią dokonaną przez Grupę Roboczą Art. 29, aby dane działanie można było uznać za „systematyczne", musi ono posiadać przynajmniej jedną z następujących cech:

- być przeprowadzane w ramach określonego systemu;
- być wcześniej zaplanowane, zorganizowane lub mieć metodyczny charakter;
- odbywać się w ramach ogólnego planu gromadzenia danych;
- być realizowane jako część strategii.

Przykłady działań, które można uznać za działania stanowiące regularne i systematyczne monitorowanie osób, których dane dotyczą: obsługa sieci telekomunikacyjnej; świadczenie usług telekomunikacyjnych; przekierowywanie wiadomości e-mail; działalność marketingowa oparta na danych; profilowanie i przyznawanie punktów na potrzeby oceny ryzyka (np. na potrzeby punktowej oceny kredytowej, ustanowienia składek ubezpieczeniowych, zwalczania nadużyć finansowych i wykrywania przypadków prania pieniędzy); śledzenie zmian lokalizacji, na przykład za pomocą aplikacji mobilnych; programy lojalnościowe; reklama behawioralna; monitorowanie samopoczucia, parametrów fizycznych i danych dotyczących zdrowia za pomocą urządzeń do noszenia na ciele; telewizja przemysłowa; urządzenia podłączone do internetu, np. inteligentne liczniki, inteligentne samochody, urządzenia związane z technologią automatyki domowej itp.

2.1.5 Szczególne kategorie danych i dane dotyczące wyroków skazujących i naruszeń prawa

Art. 37 ust. 1 lit. c) dotyczy przetwarzania szczególnych kategorii danych osobowych, o których mowa w art. 9, oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o których mowa w art. 10. Choć w literze tej pojawia się słowo „oraz", nie istnieje żadne uzasadnienie polityczne przemawiające za jednoczesnym stosowaniem tych dwóch kryteriów. Dlatego też przepis ten należy interpretować w taki sposób, jak gdyby zawierał sformułowanie „albo".

2.2. DPO podmiotu przetwarzającego

Przepisy art. 37 mają zastosowanie zarówno do administratorów[17], jak i do podmiotów przetwarzających[18], w kontekście wyznaczania DPO. W niektórych przypadkach obowiązek wyznaczenia DPO spoczywa wyłącznie na administratorze lub wyłącznie na podmiocie przetwarzającym, natomiast w innych przypadkach obowiązek ten spoczywa na obydwu z nich (w takiej sytuacji powinni oni współpracować ze sobą), w zależności od tego, który z tych podmiotów spełnia kryteria obowiązkowego wyznaczenia DPO.

Należy zwrócić uwagę na fakt, że nawet w przypadku, gdy administrator spełnia kryteria obowiązkowego wyznaczenia, obowiązek ten niekoniecznie musi rozciągać się również na jego podmiot przetwarzający. Nałożenie na podmiot przetwarzający obowiązku wyznaczenia DPO w takim przypadku można jednak uznać za dobrą praktykę.

Przykłady:

- Niewielkie przedsiębiorstwo rodzinne zajmujące się dystrybucją urządzeń gospodarstwa domowego w jednej miejscowości korzysta z usług podmiotu przetwarzającego, którego główna działalność polega na świadczeniu internetowych usług analitycznych oraz udzielaniu wsparcia w zakresie reklamy ukierunkowanej i marketingu ukierunkowanego. Działalność prowadzona przez przedsiębiorstwo rodzinne i klientów tego przedsiębiorstwa nie wiąże się z przetwarzaniem danych „na dużą skalę" z uwagi na niewielką liczbę klientów i stosunkowo ograniczony zakres prowadzonej przez nich działalności. Jednak działalność prowadzona przez podmiot przetwarzający, który posiada wielu klientów podobnych do tego małego przedsiębiorstwa, w łącznym ujęciu kwalifikuje się do uznania jej za wiążącą się z przetwarzaniem danych na dużą skalę. Podmiot przetwarzający musi zatem wyznaczyć DPO zgodnie z art. 37 ust. 1 lit. b). Jednocześnie samo przedsiębiorstwo rodzinne nie jest zobowiązane do wyznaczenia DPO.

- Średniej wielkości zakład produkcyjny zleca podwykonawstwo w zakresie usług opieki zdrowotnej w miejscu pracy zewnętrznemu podmiotowi przetwarzającemu, który posiada wielu podobnych klientów. Zgodnie z przepisami art. 37 ust. 1 lit. c) wspomniany podmiot przetwarzający jest zobowiązany wyznaczyć DPO, jeżeli przetwarza dane na dużą skalę. Sam zakład produkcyjny nie musi być jednak zobowiązany do wyznaczenia DPO.

DPO wyznaczony przez podmiot przetwarzający nadzoruje również działalność prowadzoną przez organizację podmiotu przetwarzającego w sytuacji, w której organizacja ta sama występuje w roli administratora danych (np. kwestie kadrowe, kwestie związane z IT, kwestie logistyczne).

2.3. Wyznaczenie jednego DPO dla szeregu organizacji

Zgodnie z art. 37 ust. 2 grupa przedsiębiorstw może wyznaczyć jednego DPO, o ile można będzie „łatwo nawiązać z nim kontakt z każdej jednostki organizacyjnej". Pojęcie „dostępność" odnosi się do

[17] Zgodnie z definicją przedstawioną w art. 4 pkt 7 administrator oznacza osobę lub podmiot, który ustala cele i sposoby przetwarzania.

[18] Zgodnie z definicją przedstawioną w art. 4 pkt 8 podmiot przetwarzający oznacza osobę lub podmiot, który przetwarza dane w imieniu administratora.

zadań DPO pełniącego funkcję punktu kontaktowego w odniesieniu do osób, których dane dotyczą[19], i organu nadzorczego[20], ale także – wewnętrznie – w ramach organizacji, biorąc pod uwagę fakt, że jedno z zadań DPO polega na „informowaniu administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia"[21].

Aby zapewnić dostępność DPO – niezależnie od tego, czy pełni on funkcję wewnętrzną czy zewnętrzną – należy upewnić się, że dane kontaktowe tego DPO zostały udostępnione zgodnie z wymogami RODO[22].

DPO musi mieć możliwość sprawnego komunikowania się z osobami, których dane dotyczą[23], oraz prowadzenia skutecznej współpracy[24] z odpowiednimi organami nadzorczymi, w razie potrzeby z pomocą zespołu. Oznacza to również, że komunikacja musi odbywać się w języku lub językach wykorzystywanych przez organy nadzorcze i odpowiednie osoby, których dane dotyczą. Dostępność DPO (niezależnie od tego, czy przebywa on w tym samym miejscu co pracownicy, czy też pracuje za pośrednictwem gorącej linii lub innego zabezpieczonego sposobu komunikacji) ma kluczowe znaczenie dla zagwarantowania osobom, których dane dotyczą, możliwości nawiązania kontaktu z DPO.

Zgodnie z art. 37 ust. 3 dla kilku organów lub podmiotów publicznych można wyznaczyć – z uwzględnieniem ich struktury organizacyjnej i wielkości – jednego DPO. W takim przypadku obowiązują analogiczne zasady dotyczące zasobów i komunikowania. Biorąc pod uwagę fakt, że DPO jest odpowiedzialny za wykonywanie różnego rodzaju zadań, administrator lub podmiot przetwarzający musi zapewnić, aby pojedynczy DPO – w stosownych przypadkach przy wsparciu zespołu – był w stanie skutecznie wykonywać te zadania pomimo tego, że wyznaczono go dla szeregu organów i podmiotów publicznych.

2.4. Dostępność i lokalizacja DPO

[19] Art. 38 ust. 4: „osoby, których dane dotyczą, mogą kontaktować się z inspektorem ochrony danych we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy niniejszego rozporządzenia".

[20] Art. 39 ust. 1 lit. e): „pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36, oraz w stosownych przypadkach prowadzenie konsultacji we wszystkich innych sprawach".

[21] Art. 39 ust. 1 lit. a).

[22] Zob. również sekcja 2.6 poniżej.

[23] Art. 12 ust. 1: „administrator podejmuje odpowiednie środki, aby w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem – w szczególności gdy informacje są kierowane do dziecka – udzielić osobie, której dane dotyczą, wszelkich informacji, o których mowa w art. 13 i 14, oraz prowadzić z nią wszelką komunikację na mocy art. 15–22 i 34 w sprawie przetwarzania".

[24] Art. 39 ust. 1 lit. d): „współpraca z organem nadzorczym".

Zgodnie z sekcją 4 RODO należy zapewnić dostępność DPO.

Aby zagwarantować dostępność DPO, Grupa Robocza Art. 29 zaleca, aby DPO znajdował się na terytorium Unii Europejskiej, niezależnie od tego, czy administrator lub podmiot przetwarzający ma swoją jednostkę organizacyjną w Unii Europejskiej.

Nie można jednak wykluczyć, że w niektórych przypadkach, w których administrator lub podmiot przetwarzający nie ma swojej jednostki organizacyjnej na terytorium Unii Europejskiej[25], DPO może skuteczniej wywiązywać się z powierzonych mu obowiązków w przypadku, gdy będzie znajdował się poza UE.

2.5. Wiedza fachowa i umiejętności DPO

Art. 37 ust. 5 stanowi, że DPO „jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, o których mowa w art. 39". Motyw 97 stanowi, że niezbędny poziom wiedzy fachowej należy ustalić w szczególności w świetle prowadzonych operacji przetwarzania danych oraz ochrony, której wymagają przetwarzane dane osobowe.

- **Poziom wiedzy fachowej**

Wymagany poziom wiedzy fachowej nie został precyzyjnie określony, ale musi odpowiadać on wrażliwości, złożoności i ilości danych przetwarzanych przez organizację. Na przykład, jeżeli dana czynność przetwarzania danych jest szczególnie złożona lub jeżeli zachodzi konieczność przetworzenia dużej ilości danych wrażliwych, DPO może potrzebować dodatkowej wiedzy fachowej i wsparcia. Znaczenie ma również to, czy dana organizacja systematycznie przekazuje dane osobowe poza Unię Europejską, czy też do przekazywania danych osobowych poza obszar UE dochodzi sporadycznie. Dlatego też DPO należy wybrać starannie, po należytym uwzględnieniu kwestii związanych z ochroną danych w danej organizacji.

- **Kwalifikacje zawodowe**

Choć w art. 37 ust. 5 nie określono kwalifikacji zawodowych, które należy wziąć pod uwagę przy wyznaczaniu DPO, DPO powinien posiadać wiedzę fachową w zakresie krajowych i europejskich przepisów i praktyk w dziedzinie ochrony danych, w tym dogłębną znajomość RODO. Promowanie odpowiednich i regularnych szkoleń dla DPO przez organy nadzorcze również może być przydatne.

Przydatna jest również wiedza na temat sektora, w którym prowadzona jest działalność gospodarcza, i organizacji administratora. DPO powinien również posiadać odpowiednią wiedzę na temat przeprowadzanych operacji przetwarzania danych, systemów informatycznych oraz potrzeb administratora w zakresie bezpieczeństwa danych i ochrony danych.

W przypadku organu lub podmiotu publicznego DPO powinien również posiadać gruntowną wiedzę w zakresie przepisów i procedur administracyjnych stosowanych w organizacji.

[25] Zob. art. 3 RODO dotyczący terytorialnego zakresu stosowania.

- **Umiejętność wykonania zadań**

Umiejętność wykonania zadań spoczywających na DPO należy interpretować zarówno przez pryzmat cech osobowych i wiedzy DPO, jak również jego pozycji w strukturach organizacji. Do cech osobowych zaliczyć można np. rzetelne podejście i wysoki poziom etyki zawodowej; priorytetem DPO powinno być zapewnienie przestrzegania RODO. DPO odgrywa kluczową rolę w promowaniu kultury ochrony danych w organizacji i pomaga we wdrażaniu podstawowych elementów RODO, w tym zasad przetwarzania danych[26], praw osób, których dane dotyczą[27], zasad uwzględniania ochrony danych w fazie projektowania oraz domyślnej ochrony danych[28], rejestrów czynności przetwarzania[29], bezpieczeństwa przetwarzania[30] oraz zgłaszania i informowania o przypadkach naruszenia ochrony danych[31].

- **Pełnienie funkcji DPO na podstawie umowy o świadczenie usług**

Funkcja DPO może być również pełniona na podstawie umowy o świadczenie usług zawartej z osobą fizyczną lub innym podmiotem spoza organizacji administratora / podmiotu przetwarzającego. Gdy umowę zawarto z podmiotem przetwarzającym, istotne jest, aby każdy członek organizacji sprawującej funkcję DPO spełniał wszystkie odpowiednie wymogi wskazane w sekcji 4 RODO (np. istotne jest, aby żaden z członków nie miał konfliktu interesów). Równie ważne jest, aby każdą z tych osób objąć ochroną przewidzianą w przepisach RODO (np. aby nie miało miejsca nieuzasadnione rozwiązanie umowy o świadczenie usług w zakresie pełnienia funkcji DPO, ale również aby nie miało miejsca niezgodne z prawem zwolnienie osoby będącej członkiem organizacji realizującej zadania DPO). Jednocześnie w pracy zespołowej można połączyć indywidualne atuty i umiejętności tak, aby zapewnić wydajniejszą obsługę swoich klientów.

W celu zapewnienia jasności prawa, dobrej organizacji i uniknięcia konfliktów interesów wśród członków zespołu zalecane jest wyraźne podzielenie obowiązków w ramach zespołu DPO oraz wyznaczenie jednej osoby jako wiodącej osoby kontaktowej i osoby „odpowiedzialnej" za każdego klienta. Z reguły wskazane byłoby również określenie tych kwestii w umowie o świadczenie usług.

2.6. Publikowanie danych kontaktowych DPO i zawiadamianie o tych danych

Zgodnie z art. 37 ust. 7 RODO administrator lub podmiot przetwarzający jest zobowiązany do:

- opublikowania danych kontaktowych DPO oraz
- zawiadomienia właściwych organów nadzorczych o danych kontaktowych DPO.

Celem tych wymogów jest zapewnienie, aby osoby, których dane dotyczą, (zarówno wewnątrz, jak i spoza organizacji) i organy nadzorcze mogły mieć łatwy i bezpośredni kontakt z DPO, bez konieczności kontaktowania się z innymi podmiotami organizacji. Poufność jest równie istotna: na przykład pracownicy mogą niechętnie składać skargi do DPO, jeżeli nie zostanie zagwarantowana poufność ich komunikacji.

[26] Rozdział II.
[27] Rozdział III.
[28] Art. 25.
[29] Art. 30.
[30] Art. 32.
[31] Art. 33 i 34.

DPO związany jest tajemnicą lub poufnością dotyczącą wykonywania swoich zadań – zgodnie z prawem Unii lub prawem państwa członkowskiego (art. 38 ust. 5).

Dane kontaktowe DPO powinny zawierać informacje umożliwiające osobom, których dane dotyczą, i organom nadzorczym łatwe nawiązanie kontaktu z DPO (adres korespondencyjny, dedykowany numer telefonu lub dedykowany adres e-mail). W stosownych przypadkach, do celów komunikacji ze społeczeństwem, mogą zostać zapewnione również inne środki komunikacji, np. dedykowana gorąca linia lub dedykowany formularz kontaktowy skierowany do DPO na stronie internetowej organizacji.

Zgodnie z art. 37 ust. 7 nie jest konieczne, aby publikowane dane kontaktowe zawierały imię i nazwisko DPO. Podczas gdy wskazanie tych informacji może być dobrą praktyką, to decyzja o tym, czy w określonych okolicznościach udostępnienie tych danych może być konieczne lub pomocne, zależeć będzie od administratora lub podmiotu przetwarzającego i DPO[32].

Przekazanie organowi nadzorczemu imienia i nazwiska DPO jest jednak niezbędne dla sprawowania przez DPO funkcji punktu kontaktowego pomiędzy organizacją a organem nadzorczym (art. 39 ust. 1 lit. e)).

W ramach dobrej praktyki Grupa Robocza Art. 29 zaleca również, aby organizacja podawała swoim pracownikom imię i nazwisko oraz dane kontaktowe DPO. Imię i nazwisko oraz dane kontaktowe DPO mogą zostać udostępnione wewnętrznie, np. poprzez intranet, w wewnętrznej książce telefonicznej oraz w ramach rozpisanej struktury organizacyjnej.

3 Status DPO

3.1. Udział DPO we wszystkich sprawach dotyczących ochrony danych osobowych

[32] Należy zauważyć, że w przeciwieństwie do art. 37 ust. 7 w art. 33 ust. 3 lit. b) opisującym informacje, które należy przekazać organowi nadzorczemu i osobom, których dane dotyczą, w przypadku naruszenia ochrony danych osobowych, wymaga się również podania imienia i nazwiska (a nie tylko danych kontaktowych) DPO, którego zawiadamia się o naruszeniu.

Art. 38 RODO stanowi, że „administrator oraz podmiot przetwarzający zapewniają, by inspektor ochrony danych był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych".

Istotne jest włączanie DPO lub jego zespołu we wszystkie sprawy dotyczące ochrony danych osobowych na jak najwcześniejszym etapie. W odniesieniu do oceny skutków dla ochrony danych w RODO wyraźnie przewidziano udział DPO na wczesnym etapie oraz określono, że dokonując takiej oceny skutków, administrator konsultuje się z inspektorem ochrony danych[33]. Zapewnienie informowania DPO i konsultowania się z nim od samego początku ułatwi przestrzeganie RODO, promowanie podejścia zakładającego uwzględnienie ochrony prywatności w fazie projektowania, a zatem powinno być standardową procedurą w ramach zarządzania organizacją. Ponadto ważne jest, aby DPO był postrzegany w organizacji jako partner w dyskusji i był włączany w prace grup roboczych wykonujących czynności przetwarzania danych w organizacji.

W związku z tym organizacja powinna zapewnić m.in., aby:

- DPO był zapraszany do regularnego udziału w posiedzeniach kadry kierowniczej wyższego i średniego szczebla;
- uczestniczył w podejmowaniu decyzji mających wpływ na ochronę danych. Wszystkie niezbędne informacje należy udostępnić DPO odpowiednio wcześniej, umożliwiając mu zajęcie stanowiska;
- opinia inspektora ochrony danych musi być zawsze należycie uwzględniana. W przypadku braku porozumienia Grupa Robocza Art. 29 zaleca, jako dobrą praktykę, dokumentowanie powodów niezastosowania się do porady inspektora ochrony danych;
- w przypadku stwierdzenia naruszenia ochrony danych lub innego incydentu należy niezwłocznie skonsultować się z DPO.

W razie potrzeby administrator lub podmiot przetwarzający może opracować wytyczne lub programy dotyczące ochrony danych, w których określi kiedy należy skonsultować się z DPO.

3.2. Niezbędne zasoby

W art. 38 ust. 2 RODO na organizację nakłada się obowiązek wspierania DPO „w wypełnianiu przez niego zadań [...], zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej". W szczególności należy wziąć pod uwagę następujące aspekty:

- aktywne wsparcie DPO ze strony kadry kierowniczej wyższego szczebla przy pełnieniu powierzonej mu funkcji (np. na poziomie zarządu);
- czas wystarczający do tego, by DPO mógł się wywiązać z przydzielonych mu obowiązków. Jest to szczególnie istotne, jeżeli wewnętrzny DPO jest zatrudniony w niepełnym wymiarze czasu pracy lub jeżeli zewnętrzny DPO łączy obowiązki w zakresie ochrony danych z innymi zadaniami. W przeciwnym razie sprzeczne priorytety mogłyby doprowadzić do zaniedbania obowiązków przez DPO. Bardzo ważne jest, aby DPO posiadał wystarczająco dużo czasu na

[33] Art. 35 ust. 2.

wywiązanie się ze swoich obowiązków. Dobrą praktyką jest ustalenie odsetka czasu dla DPO na wywiązanie się z obowiązków, gdy nie jest on zatrudniony w pełnym wymiarze godzin. Dobrą praktyką jest również określenie czasu potrzebnego na wypełnienie obowiązków, odpowiedniej kolejności wykonywania obowiązków DPO oraz sporządzenie planu prac w przypadku DPO (lub organizacji);

- w stosownych przypadkach wsparcie w postaci zasobów finansowych, infrastruktury (pomieszczenia, urządzenia, wyposażenie) oraz pracowników;
- oficjalne powiadomienie wszystkich pracowników o wyznaczeniu DPO w celu zapewnienia, aby wszyscy w organizacji wiedzieli o jego istnieniu i pełnionej przez niego funkcji;
- niezbędny dostęp do innych służb, np. działu zasobów ludzkich, działu prawnego, informatycznego i ochrony itd., aby DPO mógł otrzymywać niezbędne wsparcie, dane wejściowe i informacje;
- doskonalenie zawodowe. DPO musi mieć możliwość ciągłego aktualizowania wiedzy na temat postępów poczynionych w dziedzinie ochrony danych. Celem powinno być ciągłe poszerzanie wiedzy DPO oraz zachęcanie go do udziału w kursach szkoleniowych poświęconych ochronie danych i innych formach doskonalenia zawodowego, takich jak udział w prywatnych forach, warsztatach itp.;
- w zależności od rozmiaru i struktury organizacji konieczne może być powołanie zespołu DPO (DPO i jego pracowników). W takich przypadkach należy jasno określić wewnętrzną strukturę zespołu oraz zadania i obowiązki poszczególnych członków. Podobnie, jeżeli funkcję DPO pełni zewnętrzny usługodawca, zadania DPO może skutecznie wykonywać zespół osób fizycznych pracujących dla tego usługodawcy i działających pod nadzorem wyznaczonej głównej osoby odpowiedzialnej za danego klienta.

Co do zasady im bardziej skomplikowane lub tajne operacje przetwarzania danych, tym więcej środków należy przeznaczyć dla DPO. Ochrona danych musi być skuteczna i wymaga wystarczających zasobów, odpowiednich do zakresu przetwarzania danych.

3.3. Instrukcje oraz „wykonywanie obowiązków i zadań w sposób niezależny"

W art. 38 ust. 3 ustanowiono pewne podstawowe gwarancje, aby umożliwić DPO wykonywanie zadań przy zachowaniu wystarczającego stopnia autonomii w organizacji. W szczególności administratorzy / podmioty przetwarzające muszą zapewnić, by DPO „nie otrzymywał instrukcji dotyczących wykonywania [jego] zadań". W motywie 97 dodaje się, że DPO – „bez względu na to, czy są pracownikami administratora – powinni być w stanie wykonywać swoje obowiązki i zadania w sposób niezależny".

Oznacza to, że w ramach wypełniania swoich zadań zgodnie z art. 39 DPO nie może otrzymywać instrukcji dotyczących sposobu rozpatrywania sprawy, np. instrukcji dotyczących wyników, jakie należy osiągnąć, sposobu rozpatrywania skargi lub tego, czy należy przeprowadzić konsultacje z organem nadzorczym. Ponadto nie mogą zostać zobligowani do przyjęcia określonego stanowiska w sprawie przepisów dotyczących ochrony danych, np. określonej wykładni przepisów.

Niezależność DPO nie oznacza jednak, że DPO posiada uprawnienia decyzyjne wykraczające poza zadania określone w art. 39.

Administrator lub podmiot przetwarzający pozostają odpowiedzialni za przestrzeganie przepisów dotyczących ochrony danych i muszą być w stanie wykazać, że są one przestrzegane[34]. Jeżeli administrator lub podmiot przetwarzający podejmą decyzje niezgodne z RODO i zaleceniami DPO, DPO powinien mieć możliwość jasnego przedstawienia swojej odrębnej opinii najwyższemu kierownictwu i podmiotom, które podjęły takie decyzje. W tym kontekście art. 38 ust. 3 stanowi, że DPO „bezpośrednio podlega najwyższemu kierownictwu administratora lub podmiotu przetwarzającego". Taka bezpośrednia sprawozdawczość zapewnia kadrze kierowniczej wyższego szczebla (np. zarządowi) wiedzę na temat porad i zaleceń DPO w ramach wypełniania zadania polegającego na informowaniu i doradzaniu administratorowi lub podmiotowi przetwarzającemu. Kolejnym przykładem bezpośredniej sprawozdawczości jest sporządzenie rocznego sprawozdania z działalności DPO i przekazanie go najwyższemu kierownictwu.

3.4. Odwołanie lub kara za wypełnianie zadań DPO

Zgodnie z art. 38 ust. 3 DPO nie powinien być „odwoływany ani karany przez administratora ani podmiot przetwarzający za wypełnianie swoich zadań".

Wymóg ten zwiększa niezależność DPO i pozwala zapewnić im wykonywanie zadań w sposób niezależny oraz pozwala korzystać z odpowiedniej ochrony przy wykonywaniu zadań z zakresu ochrony danych.

Na mocy RODO kary są niedozwolone tylko w przypadkach, gdy są nałożone w związku z wypełnianiem przez DPO swoich zadań. Na przykład DPO może uznać określone przetwarzanie za wysoce ryzykowne i doradzić administratorowi lub podmiotowi przetwarzającemu przeprowadzenie oceny skutków dla ochrony danych, przy czym administrator lub podmiot przetwarzający może nie zgodzić się z oceną DPO. W takiej sytuacji DPO nie może zostać odwołany za udzielenie określonej porady.

Kary mogą przybierać różne formy i mogą mieć charakter bezpośredni lub pośredni. Mogą opierać się np. na braku lub opóźnieniu awansu; utrudnieniu rozwoju zawodowego; odmowie dostępu do korzyści oferowanych pozostałym pracownikom. Nieistotny jest przy tym fakt nałożenia kary, gdyż sama możliwość jej wykonania i obawa z tym związana może być wystarczająca, aby utrudnić DPO wykonanie jego zadań.

Zgodnie ze zwykłą zasadą zarządzania, a także podobnie jak w przypadku każdego innego pracownika lub wykonawcy, na podstawie i z zastrzeżeniem mających zastosowanie krajowych przepisów dotyczących zobowiązań, prawa pracy lub przepisów karnych, DPO może zostać odwołany zgodnie z prawem z przyczyn innych niż wykonywanie zadań jako DPO (np. kradzież, nękanie fizyczne i psychiczne lub molestowanie seksualne lub inne podobne wykroczenia).

W tym kontekście należy zauważyć, że w RODO nie określono jak i kiedy DPO może zostać odwołany lub zastąpiony inną osobą. Im stabilniejsza umowa z DPO i szerszy zakres ochrony przed niesprawiedliwym odwołaniem, tym większa szansa, że DPO będzie wykonywał swoje zadania w sposób niezależny. Grupa Robocza Art. 29 zaleca zatem organizacjom stosowanie takiej praktyki.

[34] Art. 5 ust. 2.

3.5. Konflikt interesów

Na mocy art. 38 ust. 6 DPO „może wykonywać inne zadania i obowiązki". Zgodnie z tym artykułem organizacja musi jednak „zapewnić, by takie zadania i obowiązki nie powodowały konfliktu interesów".

Wymóg niepowodowania konfliktu interesów jest ściśle związany z wymogiem wykonywania zadań w sposób niezależny. Chociaż DPO zezwala się na pełnienie innych funkcji, te dodatkowe zadania i obowiązki można im powierzyć tylko wówczas, gdy nie powodują konfliktów interesów. Oznacza to przede wszystkim, że DPO nie może piastować stanowiska w organizacji, które zapewniałoby mu dostęp do informacji pozwalających mu ustalić cele i sposoby przetwarzania danych osobowych. Biorąc pod uwagę specyficzną strukturę organizacyjną poszczególnych organizacji, kwestie te należy rozstrzygać w odniesieniu do indywidualnych przypadków.

Ogólnie rzecz biorąc, stanowiska w organizacji, w przypadku których dochodzi do konfliktu interesów, mogą obejmować stanowiska w strukturze kadry kierowniczej wyższego szczebla (takie jak dyrektor generalny, dyrektor ds. operacyjnych, dyrektor ds. finansowych, dyrektor ds. medycznych, kierownik departamentu marketingu, kierownik działu kadr lub kierownik departamentów IT), ale również inne stanowiska na niższych szczeblach struktury organizacyjnej, jeżeli piastowanie tych stanowisk lub pełnienie tych funkcji zapewnia możliwość ustalenia celów i sposobów przetwarzania. Ponadto konflikt interesów może powstać również wtedy, gdy np. zewnętrzny DPO zostanie poproszony o reprezentowanie administratora lub podmiotu przetwarzającego przed sądem w sprawie dotyczącej ochrony danych.

Zależnie od rodzaju działalności, rozmiaru i struktury organizacji dobrą praktyką dla administratorów lub podmiotów przetwarzających może być:

- określenie stanowisk niezgodnych z funkcją DPO;
- opracowanie wewnętrznych zasad pozwalających uniknąć konfliktu interesów;
- zapewnienie bardziej ogólnego wyjaśnienia dotyczącego konfliktów interesów;
- zadeklarowanie, że DPO nie ma konfliktu interesów w odniesieniu do pełnionej przez siebie funkcji DPO, celem zwiększenia świadomości na temat tego wymogu;
- wprowadzenie zabezpieczeń do wewnętrznych zasad organizacji oraz zapewnienie, by ogłoszenie o naborze na stanowisko DPO lub umowa o świadczenie usług były wystarczająco jasne i precyzyjne, aby uniknąć konfliktu interesów. W tym kontekście należy również mieć na uwadze, że konflikty interesów mogą przybierać różne formy w zależności od tego, czy rekrutacja na stanowisko DPO ma charakter wewnętrzny lub zewnętrzny.

4 Zadania DPO

4.1. Monitorowanie przestrzegania RODO

Na mocy art. 39 ust. 1 lit. b) na DPO nakłada się m.in. obowiązek monitorowania przestrzegania RODO. W motywie 97 określono ponadto, że „w monitorowaniu wewnętrznego przestrzegania niniejszego rozporządzenia administrator lub podmiot przetwarzający powinni być wspomagani" przez DPO.

W ramach przedmiotowych obowiązków w zakresie monitorowania przestrzegania DPO może w szczególności:

- gromadzić informacje pozwalające zidentyfikować czynności przetwarzania;
- analizować czynności przetwarzania i sprawdzać ich zgodność z przepisami rozporządzenia;
- przekazywać administratorowi lub podmiotowi przetwarzającemu informacje, udzielać im porad lub publikować skierowane do nich zalecenia.

Monitorowanie przestrzegania nie oznacza, że DPO jest osobiście odpowiedzialny w przypadkach nieprzestrzegania RODO. RODO wyraźnie stanowi, że to administrator, a nie DPO „wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać" (art. 24 ust. 1). Społeczny obowiązek zapewnienia zgodności środków w zakresie ochrony danych z przepisami rozporządzenia spoczywa na administratorze, a nie DPO.

4.2. Rola DPO w ramach oceny skutków dla ochrony danych

Zgodnie z art. 35 ust. 1 przeprowadzanie, w razie potrzeby, oceny skutków dla ochrony danych jest obowiązkiem administratora, a nie DPO. DPO może jednak odegrać bardzo ważną i użyteczną rolę we wspieraniu administratora. Zgodnie z zasadą uwzględnienia ochrony danych w fazie projektowania w art. 35 ust. 2 wyraźnie zobowiązano administratora do „konsultowania się" z DPO podczas prowadzenia oceny skutków dla ochrony danych. Z kolei zgodnie z art. 39 ust. 1 lit. c) obowiązkiem DPO jest „udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35".

Grupa Robocza Art. 29 zaleca, aby administrator zasięgnął opinii DPO m.in. w następujących kwestiach[35]:

- konieczności przeprowadzenia oceny skutków dla ochrony danych;
- metody, jaką należy zastosować przy przeprowadzaniu oceny skutków dla ochrony danych;
- ustalenia, czy ocena skutków dla ochrony danych powinna zostać przeprowadzona wewnątrz przedsiębiorstwa, czy też zlecona podmiotowi zewnętrznemu;
- ustalenia, jakie gwarancje (uwzględniając środki techniczne i organizacyjne) należy zastosować w celu ograniczenia wszelkiego rodzaju zagrożeń dla praw i interesów osób, których dane dotyczą;
- ustalenia, czy ocena skutków dla ochrony danych została przeprowadzona w prawidłowy sposób i czy jej wyniki (wnioski dotyczące tego, czy należy kontynuować przetwarzanie danych, oraz tego, jakie zabezpieczenia należy zastosować) są zgodne z przepisami RODO.

[35] W art. 39 ust. 1 wymieniono zadania DPO i określono, że DPO „ma" następujące zadania. W związku z tym nic nie stoi na przeszkodzie, aby administrator mógł przydzielić DPO zadania inne niż te wyraźnie wspomniane w art. 39 ust. 1 lub aby mógł określić te zadania bardziej szczegółowo.

Jeżeli administrator nie zgadza się z zaleceniami DPO, dokumentacja oceny skutków dla ochrony danych powinna zawierać pisemne uzasadnienie nieuwzględnienia tych zaleceń[36].

Ponadto Grupa Robocza Art. 29 zaleca, aby administrator jasno wskazał – np. w umowie z DPO, ale również w informacjach przekazywanych pracownikom, kierownikom (i innym zainteresowanym stronom) – dokładny zakres obowiązków DPO, w szczególności w kontekście przeprowadzania oceny skutków dla ochrony danych.

4.3. Współpraca z organem nadzorczym i pełnienie funkcji punktu kontaktowego

Zgodnie z art. 39 ust. 1 lit. d) i e) DPO powinien „współpracować z organem nadzorczym" i „pełnić funkcję punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach".

Zadania te odnoszą się do „pomocniczej" roli DPO, o której mowa we wstępie do niniejszych wytycznych. DPO ma pełnić funkcję punktu kontaktowego, by ułatwić organowi nadzorczemu dostęp do dokumentów i informacji w celu wypełnienia zadań, o których mowa w art. 57, oraz wykonywania uprawnień w zakresie prowadzonych postępowań, uprawnień naprawczych, uprawnień w zakresie wydawania zezwoleń oraz uprawnień doradczych, o których mowa w art. 58. Jak już wspomniano powyżej, DPO związany jest tajemnicą lub poufnością dotyczącą wykonywania swoich zadań – zgodnie z prawem Unii lub prawem państwa członkowskiego (art. 38 ust. 5). Obowiązek zachowania tajemnicy/poufności nie zabrania jednak DPO kontaktowania się z organem nadzorczym i zwracania się do niego po poradę. Art. 39 ust. 1 lit. e) stanowi, że w stosownych przypadkach DPO może konsultować się z organem nadzorczym we wszelkich innych sprawach.

4.4. Podejście oparte na analizie ryzyka

Zgodnie z art. 39 ust. 2 DPO musi wypełniać swoje zadania „z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania".

W artykule tym przywołuje się ogólną, zdroworozsądkową zasadę, którą DPO może odnieść do wielu aspektów swojej codziennej pracy. Wymaga to od DPO ustalenia priorytetów w odniesieniu do prowadzonych działań i skupienia się na aspektach pociągających za sobą większe ryzyko w zakresie ochrony danych. Nie oznacza to, że powinni oni zaniedbywać monitorowanie przestrzegania operacji przetwarzania danych o relatywnie niższym poziomie ryzyka, a jedynie wskazuje, że powinni oni skupić się przede wszystkim na obszarach podwyższonego ryzyka.

To selektywne i pragmatyczne podejście powinno ułatwić DPO udzielanie porad administratorowi w zakresie metodyki, jaką należy zastosować podczas oceny skutków dla ochrony danych, obszarów, które należy objąć wewnętrznym lub zewnętrznym audytem w zakresie ochrony danych, wewnętrznych szkoleń oferowanych pracownikom lub kierownikom odpowiedzialnym za wykonywanie czynności przetwarzania danych oraz operacji przetwarzania, na które trzeba przeznaczyć więcej czasu i zasobów.

4.5. Rola DPO w rejestrowaniu czynności przetwarzania

Zgodnie z art. 30 ust. 1 i 2 to administrator lub podmiot przetwarzający, a nie DPO „prowadzą rejestr czynności przetwarzania danych osobowych, za które odpowiadają" lub „prowadzą rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora".

W praktyce DPO często tworzą spis inwentarza i prowadzą rejestry czynności przetwarzania w oparciu o dane otrzymane od różnych działów organizacji odpowiedzialnych za przetwarzanie danych osobowych. Taka praktyka została ustalona na mocy wielu obowiązujących przepisów krajowych oraz na mocy przepisów o ochronie danych obowiązujących w instytucjach i organach UE[37].

W art. 39 ust. 1 zawarto minimalny wykaz zadań, które musi wykonać DPO. Nic nie stoi zatem na przeszkodzie, aby administrator lub podmiot przetwarzający powierzył DPO zadanie prowadzenia rejestru operacji przetwarzania pod nadzorem administratora lub podmiotu przetwarzającego. Taki rejestr powinien być traktowany jako jedno z narzędzi zapewniających DPO możliwość wywiązywania się z powierzonych mu zadań w zakresie monitorowania przestrzegania, przekazywania informacji i udzielania porad administratorowi lub podmiotowi przetwarzającemu.

W każdym razie taki rejestr, którego prowadzenia wymaga się na mocy art. 30, należy również uznać za narzędzie umożliwiające administratorowi i organowi nadzorczemu zapoznanie się na żądanie ze wszystkimi działaniami związanymi z przetwarzaniem danych osobowych, jakie prowadzi organizacja. Rejestr stanowi zatem warunek wstępny przestrzegania przepisów, a sam w sobie stanowi skuteczne narzędzie rozliczania.

[36] Art. 24 ust. 1 stanowi, że „uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem **i aby móc to wykazać**. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane".

[37] Art. 24 ust. 1 lit. d) rozporządzenia (WE) nr 45/2001.

5 ZAŁĄCZNIK – WYTYCZNE DOTYCZĄCE DPO: CO TRZEBA WIEDZIEĆ?

Celem niniejszego załącznika jest udzielenie odpowiedzi – w prostej i przejrzystej formie – na niektóre kluczowe pytania, jakie organizacje mogą zadawać w związku z ustanowieniem nowych wymogów w zakresie wyznaczania DPO w ogólnym rozporządzeniu o ochronie danych (RODO).

Wyznaczenie DPO

1 Które organizacje są zobowiązane wyznaczyć DPO?

Wyznaczenie DPO jest obowiązkowe:

- jeżeli przetwarzania dokonują organ lub podmiot publiczny (niezależnie od rodzaju przetwarzanych danych);
- jeżeli główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę;
- jeżeli główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa.

Należy zwrócić uwagę na fakt, że przepisy obowiązujące w Unii lub w państwach członkowskich mogą wymagać wyznaczenia DPO również w innych sytuacjach. Ponadto nawet jeżeli wyznaczenie DPO nie jest obowiązkowe, organizacje mogą niekiedy uznać za przydatne wyznaczenie DPO na zasadzie dobrowolności. Grupa Robocza Art. 29 zachęca do podejmowania dobrowolnych wysiłków w tym obszarze. Jeżeli organizacja wyznaczyła DPO na zasadzie dobrowolności, kwestie związane z wyznaczeniem takiego DPO, jego statusem i spoczywającymi na nim obowiązkami będą regulowały te same wymogi, jak gdyby został on wyznaczony w ramach obowiązku wyznaczenia DPO.

Źródło: art. 37 ust. 1 RODO.

2 Co oznacza pojęcie „główna działalność"?

„Główna działalność" oznacza kluczowe operacje, które administrator lub podmiot przetwarzający podejmują, aby osiągnąć swoje cele. Pojęcie to obejmuje również wszystkie czynności, w przypadku których przetwarzanie danych stanowi nieodłączny element działalności prowadzonej przez administratora lub podmiot przetwarzający. Na przykład przetwarzanie danych dotyczących zdrowia, takich jak dokumentacja medyczna pacjenta, powinno zostać uznane za jeden z elementów głównej działalności każdego szpitala, dlatego też szpitale są zobowiązane wyznaczyć DPO.

Wszystkie organizacje podejmują natomiast określonego rodzaju działania wspierające, na przykład przy wypłacaniu wynagrodzeń swoim pracownikom lub przy podejmowaniu standardowych czynności w zakresie wsparcia IT. Są to przykłady funkcji wspierających, które mają kluczowe znaczenie dla głównej działalności lub głównego obszaru zainteresowań danej organizacji. Choć działania w tym zakresie są niezbędne i kluczowe, zazwyczaj uznaje się je za działania pomocnicze, a nie za element głównej działalności.

Źródło: art. 37 ust. 1 lit. b) i c) RODO.

3 Co oznacza pojęcie „na dużą skalę"?

W RODO nie zawarto definicji pojęcia „przetwarzanie na dużą skalę". Grupa Robocza Art. 29 zaleca, aby przy ustalaniu, czy przetwarzanie danych odbywa się na dużą skalę, wziąć pod uwagę w szczególności następujące czynniki:

- liczbę osób, których dane dotyczą – wyrażoną jako konkretna wartość albo jako odsetek populacji odniesienia;
- ilość danych lub zakres poszczególnych przetwarzanych pozycji danych;
- czas trwania lub trwałość czynności przetwarzania danych;
- zakres geograficzny czynności przetwarzania.

Przykłady przetwarzania na dużą skalę obejmują:

- przetwarzanie danych pacjentów przez szpital w ramach prowadzonej przez niego działalności;
- przetwarzanie danych o podróży osób fizycznych korzystających z miejskiego systemu transportu publicznego (np. śledzenie za pośrednictwem biletów elektronicznych);
- przetwarzanie danych określających położenie geograficzne klientów międzynarodowej sieci restauracji typu fast-food w czasie rzeczywistym do celów statystycznych przez podmiot przetwarzający specjalizujący się w podejmowaniu takich działań;
- przetwarzanie danych klientów przez zakład ubezpieczeń lub bank w ramach prowadzonej przez te podmioty działalności gospodarczej;
- przetwarzanie danych osobowych przez wyszukiwarkę internetową na potrzeby reklamy behawioralnej;
- przetwarzanie danych (treść, przepływ danych, lokalizacja) przez dostawców usług telefonicznych lub internetowych.

Przykłady działań, które nie stanowią przetwarzania na dużą skalę:

- przetwarzanie danych pacjenta przez pojedynczego lekarza;
- przetwarzanie danych osobowych dotyczących wyroków skazujących i naruszeń prawa przez pojedynczego prawnika.

Źródło: art. 37 ust. 1 lit. b) i c) RODO.

4 Co oznacza pojęcie „regularne i systematyczne monitorowanie"?

Choć pojęcie regularnego i systematycznego monitorowania osób, których dane dotyczą, nie zostało zdefiniowane w RODO, w oczywisty sposób obejmuje ono wszystkie formy śledzenia i profilowania w internecie na potrzeby reklamy behawioralnej. Pojęcie monitorowania nie ogranicza się jednak wyłącznie do aktywności prowadzonej w internecie.

Przykłady działań, które można uznać za działania stanowiące regularne i systematyczne monitorowanie osób, których dane dotyczą: obsługa sieci telekomunikacyjnej; świadczenie usług telekomunikacyjnych; przekierowywanie wiadomości e-mail; działalność marketingowa oparta na danych; profilowanie i przyznawanie punktów na potrzeby oceny ryzyka (np. na potrzeby punktowej oceny kredytowej, ustanowienia składek ubezpieczeniowych, zwalczania nadużyć finansowych i wykrywania przypadków prania pieniędzy); śledzenie zmian lokalizacji, na przykład za pomocą aplikacji mobilnych; programy lojalnościowe; reklama behawioralna; monitorowanie samopoczucia, parametrów fizycznych i danych dotyczących zdrowia za pomocą urządzeń do noszenia na ciele;

telewizja przemysłowa; urządzenia podłączone do internetu, np. inteligentne liczniki, inteligentne samochody, urządzenia związane z technologią automatyki domowej itp.

Zgodnie z wykładnią dokonaną przez Grupę Roboczą Art. 29, aby dane działanie można było uznać za „regularne", musi ono posiadać przynajmniej jedną z następujących cech:

- być aktualnie w toku lub być podejmowane w regularnych odstępach czasu w danym okresie;
- być prowadzone cyklicznie lub powtarzać się w określonych momentach;
- być prowadzone stale lub okresowo.

Zgodnie z wykładnią dokonaną przez Grupę Roboczą Art. 29, aby dane działanie można było uznać za „systematyczne", musi ono posiadać przynajmniej jedną z następujących cech:

- być przeprowadzane w ramach określonego systemu;
- być wcześniej zaplanowane, zorganizowane lub mieć metodyczny charakter;
- odbywać się w ramach ogólnego planu gromadzenia danych;
- być realizowane jako część strategii.

Źródło: art. 37 ust. 1 lit. b) RODO.

5 Czy organizacje mogą wspólnie wyznaczyć DPO? Jeżeli tak, to na jakich warunkach?

Tak. Grupa przedsiębiorstw może wyznaczyć jednego DPO, o ile można będzie „łatwo nawiązać z nim kontakt z każdej jednostki organizacyjnej". Pojęcie „dostępność" odnosi się do zadań DPO pełniącego funkcję punktu kontaktowego w odniesieniu do osób, których dane dotyczą, organów nadzorczych, a także – wewnętrznie – w ramach organizacji. Aby zapewnić dostępność DPO – niezależnie od tego, czy pełni on funkcję wewnętrzną czy zewnętrzną – należy upewnić się, że dane kontaktowe tego DPO zostały udostępnione. DPO musi mieć możliwość sprawnego komunikowania się z osobami, których dane dotyczą, oraz prowadzenia skutecznej współpracy z odpowiednimi organami nadzorczymi, w razie potrzeby z pomocą zespołu. Oznacza to, że komunikacja musi odbywać się w języku lub językach wykorzystywanych przez organy nadzorcze i odpowiednie osoby, których dane dotyczą. Dostępność DPO (niezależnie od tego, czy przebywa on w tym samym miejscu co pracownicy, czy też pracuje za pośrednictwem gorącej linii lub innego zabezpieczonego sposobu komunikacji) ma kluczowe znaczenie dla zagwarantowania osobom, których dane dotyczą, możliwości nawiązania kontaktu z DPO.

Dla kilku organów lub podmiotów publicznych można wyznaczyć – z uwzględnieniem ich struktury organizacyjnej i wielkości – jednego DPO. W takim przypadku obowiązują analogiczne zasady dotyczące zasobów i komunikowania. Biorąc pod uwagę fakt, że DPO jest odpowiedzialny za wykonywanie różnego rodzaju zadań, administrator lub podmiot przetwarzający musi zapewnić, aby pojedynczy DPO – w stosownych przypadkach przy wsparciu zespołu – był w stanie skutecznie wykonywać te zadania pomimo tego, że wyznaczono go dla szeregu organów i podmiotów publicznych.

Źródło: art. 37 ust. 2 i 3 RODO.

6 Gdzie powinna znajdować się siedziba DPO?

Aby zagwarantować dostępność DPO, Grupa Robocza Art. 29 zaleca, aby DPO znajdował się na terytorium Unii Europejskiej, niezależnie od tego, czy administrator lub podmiot przetwarzający ma swoją jednostkę organizacyjną w Unii Europejskiej. Nie można jednak wykluczyć, że w niektórych

przypadkach, w których administrator lub podmiot przetwarzający nie ma swojej jednostki organizacyjnej na terytorium Unii Europejskiej, DPO może skutecznie wywiązywać się z powierzonych mu obowiązków w przypadku, gdy będzie znajdował się poza UE.

7 Czy można wyznaczyć zewnętrznego DPO?

Tak. DPO może być członkiem personelu administratora lub podmiotu przetwarzającego (wewnętrzny DPO) lub „wykonywać zadania na podstawie umowy o świadczenie usług". Oznacza to, że DPO może być zewnętrznym DPO – w takim przypadku pełni on powierzoną mu funkcję na podstawie umowy o świadczenie usług zawartej z daną osobą fizyczną lub organizacją.

Jeżeli funkcję DPO pełni zewnętrzny usługodawca, zadania DPO może skutecznie wykonywać zespół osób fizycznych pracujących dla tego usługodawcy działających pod nadzorem wyznaczonej głównej osoby odpowiedzialnej za kontakty oraz „osoby odpowiedzialnej" za danego klienta. W takiej sytuacji kluczowe znaczenie ma zagwarantowanie, aby wszyscy członkowie organizacji zewnętrznej pełniący funkcje DPO spełniali obowiązujące wymogi RODO.

W wytycznych zaleca się wyraźne podzielenie obowiązków w ramach zespołu zewnętrznego DPO i wyznaczenie jednej osoby jako osoby odpowiedzialnej za kontakty oraz za danego klienta w umowie o świadczenie usług w celu zapewnienia jasności prawa i dobrej organizacji oraz w celu uniknięcia konfliktów interesów wśród członków zespołu.

Źródło: art. 37 ust. 6 RODO.

8 Jakie kwalifikacje zawodowe powinien posiadać DPO?

DPO jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań.

Niezbędny poziom wiedzy fachowej należy ustalić w szczególności w świetle prowadzonych operacji przetwarzania danych oraz ochrony, której wymagają przetwarzane dane osobowe. Na przykład, jeżeli dana czynność przetwarzania danych jest szczególnie złożona lub jeżeli zachodzi konieczność przetworzenia dużej ilości danych wrażliwych, DPO może potrzebować dodatkowej wiedzy fachowej i wsparcia.

Odpowiednie umiejętności i odpowiednia wiedza fachowa obejmują:

- wiedzę fachową w zakresie krajowych i europejskich przepisów i praktyk w dziedzinie ochrony danych, w tym dogłębną znajomość RODO;
- wiedzę na temat przeprowadzanych operacji przetwarzania;
- znajomość technologii informacyjnych i zasad bezpieczeństwa danych;
- wiedzę na temat sektora, w którym prowadzona jest działalność gospodarcza, oraz na temat danej organizacji;
- umiejętność promowania kultury ochrony danych w organizacji.

Źródło: art. 37 ust. 5 RODO.

Status DPO

9 Jakie zasoby administrator lub podmiot przetwarzający powinni zapewnić DPO?

DPO musi posiadać zasoby niezbędne do wykonywania swoich zadań.

W zależności od specyfiki operacji przetwarzania oraz działalności prowadzonej przez organizację i jej wielkości DPO należy zapewnić:

- aktywne wsparcie ze strony kadry kierowniczej wyższego szczebla przy pełnieniu powierzonej mu funkcji;
- czas wystarczający do tego, by mógł się on wywiązać z przydzielonych mu obowiązków;
- w stosownych przypadkach wsparcie w postaci zasobów finansowych, infrastruktury (pomieszczenia, urządzenia, wyposażenie) oraz pracowników;
- oficjalne powiadomienie wszystkich pracowników o jego wyznaczeniu;
- dostęp do innych służb w ramach organizacji, aby mógł on otrzymywać niezbędne wsparcie, dane wejściowe lub informacje;
- doskonalenie zawodowe.

Źródło: art. 38 ust. 2 RODO.

10 Jakie gwarancje należy ustanowić, aby zapewnić DPO możliwość samodzielnego wykonywania powierzonych mu zadań? Co oznacza pojęcie „konflikt interesów"?

Istnieje szereg gwarancji zapewniających DPO możliwość samodzielnego wykonywania powierzonych mu zadań:

- zakaz instruowania DPO w zakresie sposobu wykonywania powierzonych mu zadań przez administratorów lub podmioty przetwarzające;
- zakaz odwołania DPO ze stanowiska lub nałożenia na niego sankcji przez administratora w związku z wykonywanymi przez niego zadaniami;
- brak konfliktu interesów, jeżeli chodzi o inne potencjalne zadania i obowiązki.

Inne zadania i obowiązki DPO nie mogą prowadzić do konfliktu interesów. Oznacza to, po pierwsze, że DPO nie może piastować stanowiska w organizacji, które zapewniałoby mu dostęp do informacji pozwalających mu ustalić cele i sposoby przetwarzania danych osobowych. Biorąc pod uwagę specyficzną strukturę organizacyjną poszczególnych organizacji, kwestie te należy rozstrzygać w odniesieniu do indywidualnych przypadków.

Ogólnie rzecz biorąc, stanowiska w organizacji, w przypadku których dochodzi do konfliktu interesów, mogą obejmować stanowiska w strukturze kadry kierowniczej wyższego szczebla (takie jak dyrektor generalny, dyrektor ds. operacyjnych, dyrektor ds. finansowych, dyrektor ds. medycznych, kierownik departamentu marketingu, kierownik działu kadr lub kierownik departamentów IT), ale również inne stanowiska na niższych szczeblach struktury organizacyjnej, jeżeli piastowanie tych stanowisk lub pełnienie tych funkcji zapewnia możliwość ustalenia celów i sposobów przetwarzania. Ponadto konflikt interesów może powstać również wtedy, gdy np. zewnętrzny DPO zostanie

poproszony o reprezentowanie administratora lub podmiotu przetwarzającego przed sądem w sprawie dotyczącej ochrony danych.

Źródło: art. 38 ust. 3 i 6 RODO.

Zadania DPO

11 Co oznacza termin „monitorowanie przestrzegania"?

W ramach przedmiotowych obowiązków w zakresie monitorowania przestrzegania DPO może w szczególności:

- gromadzić informacje pozwalające zidentyfikować czynności przetwarzania;
- analizować czynności przetwarzania i sprawdzać ich zgodność z przepisami rozporządzenia;
- przekazywać administratorowi lub podmiotowi przetwarzającemu informacje, udzielać im porad lub publikować skierowane do nich zalecenia.

Źródło: art. 39 ust. 1 lit. b) RODO.

12 Czy DPO ponosi osobistą odpowiedzialność za przypadki naruszenia wymogów dotyczących ochrony danych?

Nie, DPO nie ponosi osobistej odpowiedzialności za przypadki naruszenia wymogów dotyczących ochrony danych. Obowiązek zagwarantowania i wykazania, iż przetwarzanie danych odbywa się zgodnie z przepisami rozporządzenia, spoczywa na administratorze lub podmiocie przetwarzającym. Obowiązek zapewnienia zgodności środków w zakresie ochrony danych z przepisami rozporządzenia spoczywa na administratorze lub podmiocie przetwarzającym.

13 Jaką rolę pełni DPO w procesie oceny skutków dla ochrony danych i rejestru czynności przetwarzania danych osobowych?

Jeżeli chodzi o ocenę skutków dla ochrony danych, administrator lub podmiot przetwarzający powinien zasięgnąć opinii DPO m.in. w następujących kwestiach:

- konieczności przeprowadzenia oceny skutków dla ochrony danych;
- metody, jaką należy zastosować przy przeprowadzaniu oceny skutków dla ochrony danych;
- ustalenia, czy ocena skutków dla ochrony danych powinna zostać przeprowadzona wewnątrz przedsiębiorstwa, czy też zlecona podmiotowi zewnętrznemu;
- ustalenia, jakie gwarancje (uwzględniając środki techniczne i organizacyjne) należy zastosować w celu ograniczenia wszelkiego rodzaju zagrożeń dla praw i interesów osób, których dane dotyczą;
- ustalenia, czy ocena skutków dla ochrony danych została przeprowadzona w prawidłowy sposób i czy jej wyniki (wnioski dotyczące tego, czy należy kontynuować przetwarzanie danych, oraz tego, jakie zabezpieczenia należy zastosować) są zgodne z wymogami w zakresie ochrony danych.

Jeżeli chodzi o rejestry czynności przetwarzania, odpowiedzialność za monitorowanie procesu rejestrowania operacji przetwarzania spoczywa na administratorze lub podmiocie przetwarzającym, a nie na DPO. Nic nie stoi jednak na przeszkodzie, aby administrator lub podmiot przetwarzający powierzył DPO zadanie prowadzenia rejestrów operacji przetwarzania pod nadzorem administratora lub podmiotu przetwarzającego. Takie rejestry powinny być traktowane jako jedno z narzędzi zapewniających DPO możliwość wywiązywania się z powierzonych mu zadań w zakresie monitorowania przestrzegania, przekazywania informacji i udzielania porad administratorowi lub podmiotowi przetwarzającemu.

Źródło: art. 39 ust. 1 lit. c) i art. 30 RODO.

Sporządzono w Brukseli dnia 13 grudnia 2016 r.

W imieniu Grupy Roboczej
Przewodnicząca

Isabelle FALQUE-PIERROTIN

Ostatnio zmienione i przyjęte w dniu 5 kwietnia 2017 r.

W imieniu Grupy Roboczej
Przewodnicząca

Isabelle FALQUE-PIERROTIN

GRUPA ROBOCZA ART. 29

16/PL
WP 244 rev.01

Wytyczne dotyczące ustalania wiodącego organu nadzorczego właściwego dla administratora lub podmiotu przetwarzającego

Przyjęte w dniu 13 grudnia 2016 r.
Ostatnio zmienione i przyjęte w dniu 5 kwietnia 2017 r.

Grupa Robocza została powołana na mocy art. 29 dyrektywy 95/46/WE. Jest ona niezależnym europejskim organem doradczym w zakresie ochrony danych i prywatności. Zadania Grupy zostały określone w przepisach art. 30 dyrektywy 95/46/WE i art. 15 dyrektywy 2002/58/WE.

Obsługę sekretariatu zapewnia Dyrekcja C (Prawa podstawowe i praworządność) Dyrekcji Generalnej ds. Sprawiedliwości i Konsumentów Komisji Europejskiej, B-1049 Bruksela, Belgia, biuro nr MO59 05/35.

Strona internetowa: http://ec.europa.eu/justice/data-protection/index_en.htm

Spis treści

1. Ustalanie właściwego wiodącego organu nadzorczego: kluczowe pojęcia. 3
1.1 „Transgraniczne przetwarzanie danych osobowych” 3
1.1.1 „Znacznie wpływa” 3
1.2 Wiodący organ nadzorczy 4
1.3 Główna jednostka organizacyjna 5
2. Kroki w kierunku ustalenia wiodącego organu nadzorczego 5
2.1 Ustalenie „głównej jednostki organizacyjnej” w przypadku administratorów 5
2.1.1 Kryteria ustalania głównej jednostki organizacyjnej administratora w przypadkach, gdy nie jest to miejsce jego centralnej administracji w UE. 7
2.1.2 Grupy przedsiębiorstw 8
2.1.3 Współadministratorzy danych 8
2.2 Przypadki graniczne 9
2.3 Podmiot przetwarzający 10
3. Inne istotne kwestie 10
3.1 Rola „organu nadzorczego, którego sprawa dotyczy” 10
3.2 Lokalne przetwarzanie 11
3.3 Przedsiębiorstwa nieposiadające jednostki organizacyjnej w UE 12
ZAŁĄCZNIK – Pytania mające na celu pomoc w ustaleniu wiodącego organu nadzorczego 12

1. Ustalanie właściwego wiodącego organu nadzorczego: kluczowe pojęcia.

1.1 „Transgraniczne przetwarzanie danych osobowych”

Ustalenie wiodącego organu nadzorczego jest istotne wyłącznie wówczas, gdy administrator lub podmiot przetwarzający dokonuje transgranicznego przetwarzania danych osobowych. W art. 4 pkt 23 ogólnego rozporządzenia o ochronie danych (RODO) zdefiniowano „transgraniczne przetwarzanie” jako:

- „przetwarzanie danych osobowych, które odbywa się w Unii w ramach działalności jednostek organizacyjnych w więcej, niż jednym państwie członkowskim administratora lub podmiotu przetwarzającego w Unii posiadającego jednostki organizacyjne w więcej niż jednym państwie członkowskim; albo

- przetwarzanie danych osobowych, które odbywa się w Unii w ramach działalności pojedynczej jednostki organizacyjnej administratora lub podmiotu przetwarzającego w Unii, ale które znacznie wpływa lub może znacznie wpłynąć na osoby, których dane dotyczą, w więcej niż jednym państwie członkowskim”.

Oznacza to, że jeżeli przykładowo dana organizacja ma jednostki organizacyjne we Francji i w Rumunii, a przetwarzanie danych osobowych odbywa się w ramach ich działalności, tego rodzaju przetwarzanie określa się mianem transgranicznego przetwarzania.

Ewentualnie organizacja może dokonywać czynności przetwarzania wyłącznie w ramach działalności jednostki organizacyjnej we Francji. Jeżeli jednak czynność ta znacznie wpływa lub może znacznie wpłynąć na osoby, których dane dotyczą, we Francji i w Rumunii, tego rodzaju czynność również będzie stanowiła transgraniczne przetwarzanie.

1.1.1 „Znacznie wpływa”

W RODO nie zdefiniowano określeń „znacznie” ani „wpływa”. Takie brzmienie miało na celu zapewnienie, by nie wszystkie czynności przetwarzania mające *jakikolwiek* skutek i odbywające się w ramach działalności pojedynczej jednostki organizacyjnej były objęte zakresem definicji „transgranicznego przetwarzania”.

Najodpowiedniejsze zwykłe znaczenia terminu „znaczny” (ang. *substantial*) w języku angielskim są następujące: „w dużej lub znaczącej ilości bądź o dużym lub znaczącym rozmiarze; spory, dość duży” lub „mający solidną wartość, rzeczywiście istotny; istotny; znaczący, ważny” (Oxford English Dictionary).

Najodpowiedniejsze znaczenie czasownika „wpływać” (ang. *affect*) jest następujące: „mieć wpływ na” lub „wywierać istotny wpływ na”. Powiązany z tym rzeczownik „skutek” (ang. *effect*) oznacza, między innymi, „wynik” lub „konsekwencję” (Oxford English Dictionary). Sugeruje to, że aby przetwarzanie danych *wpłynęło* na kogoś, musi na niego w pewien sposób oddziaływać. Przetwarzanie, które nie ma znacznego wpływu na osoby fizyczne, nie wchodzi w zakres drugiej części definicji „transgranicznego przetwarzania”. Byłoby jednak objęte zakresem pierwszej części definicji w przypadku, gdy przetwarzanie danych osobowych odbywa się w ramach działalności jednostek organizacyjnych w więcej niż jednym państwie członkowskim administratora lub podmiotu przetwarzającego w Unii posiadającego jednostki organizacyjne w więcej niż jednym państwie członkowskim.

Aby uznać, że przetwarzanie jest objęte zakresem drugiej części definicji, wystarczy, by istniało prawdopodobieństwo znacznego wpływu, nawet jeżeli wpływ ten w rzeczywistości nie jest znaczny. Należy zauważyć, że określenie „może" (ang. *likely to*) nie oznacza, że istnieje odległa w czasie możliwość znacznego wpływu. Znaczny wpływ musi być bardziej prawdopodobny niż nieprawdopodobny. Z drugiej strony oznacza to również, że nie musi istnieć rzeczywisty wpływ na osoby fizyczne: prawdopodobieństwo znacznego wpływu wystarcza do uznania przetwarzania za objęte zakresem definicji „transgranicznego przetwarzania".

Fakt, że operacja przetwarzania danych może obejmować przetwarzanie szeregu – nawet znacznej ilości – danych osobowych osób fizycznych, w szeregu państw członkowskich, niekoniecznie oznacza, że przetwarzanie ma lub może mieć znaczny wpływ. Przetwarzanie, które nie wywiera znacznego wpływu, nie stanowi transgranicznego przetwarzania do celów drugiej części definicji, niezależnie od tego, na ile osób fizycznych wpływa.

Organy nadzorcze dokonają wykładni określenia „znacznie wpływa" w poszczególnych przypadkach. Należy uwzględnić kontekst przetwarzania, rodzaj danych, cel przetwarzania danych oraz czynniki, takie jak fakt, czy przetwarzanie:

- wyrządza lub może wyrządzić szkodę osobom fizycznym, naraża lub może je narazić na straty lub powoduje lub może spowodować stres u osób fizycznych;
- wywiera lub może wywierać faktyczne skutki w postaci ograniczenia praw lub pozbawienia możliwości;
- wpływa lub może wpływać na zdrowie, pomyślność lub spokój umysłu osób fizycznych;
- wpływa lub może wpływać na status finansowy lub gospodarczy osób fizycznych lub ich sytuację;
- naraża osoby fizyczne na dyskryminację lub niesprawiedliwe traktowanie;
- obejmuje analizę szczególnych kategorii danych osobowych lub innych danych wrażliwych, w szczególności danych osobowych dzieci;
- powoduje lub może spowodować znaczną zmianę zachowania osób fizycznych;
- ma mało prawdopodobne, nieoczekiwane lub niepożądane konsekwencje dla osób fizycznych;
- powoduje zakłopotanie lub ma inne negatywne skutki, w tym naruszenie dobrego imienia; lub
- obejmuje przetwarzanie szerokiego zakresu danych osobowych.

Ponadto test „znacznego wpływu" ma na celu zapewnienie, by organy nadzorcze były zobowiązane do oficjalnej współpracy z wykorzystaniem mechanizmu spójności określonego w RODO wyłącznie „w przypadkach, gdy organ nadzorczy zamierza przyjąć środek mający wywoływać skutki prawne w odniesieniu do operacji przetwarzania, które znacznie wpływają na istotną liczbę osób, których dane dotyczą, w kilku państwach członkowskich". (motyw 135)

1.2 Wiodący organ nadzorczy

Najprościej mówiąc, „wiodący organ nadzorczy" to organ, na którym spoczywa główna odpowiedzialność za prowadzenie postępowań w przedmiocie transgranicznych czynności

przetwarzania danych, na przykład gdy osoba, której dane dotyczą, wnosi skargę dotyczącą przetwarzania jej danych osobowych.

Wiodący organ nadzorczy będzie koordynować postępowania, w które zaangażowane są inne organy nadzorcze, „których sprawa dotyczy".

Ustalenie wiodącego organu nadzorczego zależy od ustalenia lokalizacji „głównej jednostki organizacyjnej" lub „pojedynczej jednostki organizacyjnej" administratora w UE. Zgodnie z art. 56 RODO:

- „organ nadzorczy głównej lub pojedynczej jednostki organizacyjnej administratora lub podmiotu przetwarzającego jest właściwy do podejmowania działań jako wiodący organ nadzorczy – zgodnie z procedurą [współpracy] przewidzianą w art. 60 – względem transgranicznego przetwarzania dokonywanego przez tego administratora lub ten podmiot przetwarzający".

1.3 Główna jednostka organizacyjna

Art. 4 pkt 16 RODO stanowi, że „główna jednostka organizacyjna" oznacza:

- „jeżeli chodzi o administratora posiadającego jednostki organizacyjne w więcej niż jednym państwie członkowskim – miejsce, w którym znajduje się jego **centralna administracja** w Unii, a jeżeli **decyzje co do celów i sposobów** przetwarzania danych osobowych zapadają w innej jednostce organizacyjnej tego administratora w Unii i ta jednostka organizacyjna **ma prawo nakazać wykonanie takich decyzji,** to za główną jednostkę organizacyjną uznaje się jednostkę organizacyjną, w której zapadają takie decyzje;

- jeżeli chodzi o podmiot przetwarzający posiadający jednostki organizacyjne w więcej niż jednym państwie członkowskim – miejsce, w którym znajduje się jego centralna administracja w Unii lub, w przypadku gdy podmiot przetwarzający nie ma centralnej administracji w Unii – jednostkę organizacyjną podmiotu przetwarzającego w Unii, w której odbywają się główne czynności przetwarzania w ramach działalności jednostki organizacyjnej podmiotu przetwarzającego, w zakresie w jakim podmiot przetwarzający podlega szczególnym obowiązkom na mocy niniejszego rozporządzenia".

2. Kroki w kierunku ustalenia wiodącego organu nadzorczego

2.1 Ustalenie „głównej jednostki organizacyjnej" w przypadku administratorów

W celu ustalenia, gdzie znajduje się główna jednostka organizacyjna, w pierwszej kolejności konieczne jest ustalenie, gdzie znajduje się centralna administracja administratora danych w UE, o ile tego rodzaju administracja istnieje[1]. Zgodnie z podejściem przyjętym w RODO centralna administracja w UE to miejsce, w którym zapadają decyzje co do celów i sposobów

[1] RODO ma znaczenie dla EOG i będzie miało zastosowanie po jego włączeniu do Porozumienia EOG. RODO jest obecnie poddawane kontroli w celu odnośnego włączenia, zob. http://www.efta.int/eea-lex/32016R0679

przetwarzania danych osobowych, przy czym miejsce to ma prawo nakazać wykonanie takich decyzji.

Istota zasady wiodącego organu nadzorczego określona w RODO jest taka, że nadzór nad transgranicznym przetwarzaniem powinien być sprawowany tylko przez jeden organ nadzorczy w UE. W przypadkach, w których w centralnej administracji w UE podejmowane są decyzje dotyczące różnych czynności transgranicznego przetwarzania, jeden wiodący organ nadzorczy będzie właściwy w zakresie różnych czynności przetwarzania danych dokonywanych przez przedsiębiorstwo wielonarodowe. Mogą jednak wystąpić przypadki, w których jednostka organizacyjna inna niż miejsce centralnej administracji podejmuje niezależne decyzje co do celów i sposobów danej czynności przetwarzania. Oznacza to, że mogą mieć miejsce sytuacje, w których będzie można ustalić właściwość więcej niż jednego wiodącego organu nadzorczego, tj. w przypadkach, gdy przedsiębiorstwo wielonarodowe postanawia utworzyć odrębne ośrodki podejmowania decyzji, w różnych państwach, w odniesieniu do różnych czynności przetwarzania.

Warto przypomnieć, że gdy przedsiębiorstwo wielonarodowe centralizuje proces podejmowania wszystkich decyzji co do celów i sposobów czynności przetwarzania w jednej ze swoich jednostek organizacyjnych w UE (przy czym ta jednostka organizacyjna ma prawo nakazać wykonanie takich decyzji), wyłącznie jeden wiodący organ nadzorczy zostanie ustalony jako właściwy dla tego przedsiębiorstwa wielonarodowego.

W takich sytuacjach kluczowe będzie, aby przedsiębiorstwa jednoznacznie określiły, gdzie podejmowane są decyzje dotyczące celu i sposobów przetwarzania. Właściwa identyfikacja głównej jednostki organizacyjnej leży w interesie administratorów i podmiotów przetwarzających, ponieważ zapewnia jasność co do tego, z którym organem nadzorczym będą oni mieli styczność, jeżeli chodzi o różne obowiązki w zakresie przestrzegania przepisów ustanowionych w RODO. Należą do nich w stosownych przypadkach: wyznaczenie inspektora ochrony danych lub konsultacje w sprawie czynności przetwarzania niosącej ryzyko, którego administrator nie może zminimalizować przy wykorzystaniu rozsądnych środków. Właściwe przepisy RODO mają umożliwić realizację tych zadań dotyczących zapewnienia przestrzegania przepisów.

Ilustrują to poniższe przykłady:

Przykład 1: Detalista w branży spożywczej ma siedzibę główną (tj. „miejsce centralnej administracji") w Rotterdamie w Holandii. Posiada jednostki organizacyjne w różnych innych państwach UE, które kontaktują się tam z osobami fizycznymi. Wszystkie jednostki organizacyjne korzystają z tego samego oprogramowania do przetwarzania danych osobowych konsumentów do celów marketingowych. Wszystkie decyzje dotyczące celów i sposobów przetwarzania danych osobowych konsumentów do celów marketingowych podejmowane są w siedzibie głównej w Rotterdamie. Oznacza to, że wiodącym organem nadzorczym właściwym dla przedsiębiorstwa w przypadku tej czynności transgranicznego przetwarzania jest organ nadzorczy w Holandii.

Przykład 2: Bank ma siedzibę główną we Frankfurcie i wszystkie[2] jego czynności przetwarzania bankowego są organizowane z tego miejsca, jednak jego dział ubezpieczeń znajduje się w Wiedniu. Jeżeli jednostka organizacyjna w Wiedniu jest uprawniona do decydowania o wszystkich czynnościach przetwarzania danych ubezpieczeniowych oraz do wykonywania tych decyzji w odniesieniu do całej UE, zgodnie z art. 4 pkt 16 RODO austriacki organ nadzorczy jest wiodącym organem nadzorczym właściwym w zakresie transgranicznego przetwarzania danych osobowych do celów ubezpieczeniowych, a organy niemieckie (organ nadzorczy Hesji) nadzorują przetwarzanie danych osobowych do celów bankowych niezależnie od tego, gdzie znajdują się klienci[3].

2.1.1 Kryteria ustalania głównej jednostki organizacyjnej administratora w przypadkach, gdy nie jest to miejsce jego centralnej administracji w UE.

Motyw 36 RODO stanowi pomoc w interpretacji głównego czynnika, który stosuje się w celu ustalenia głównej jednostki organizacyjnej administratora, jeżeli nie ma zastosowania kryterium centralnej administracji. Wiąże się to z ustaleniem, gdzie odbywa się skuteczne i faktycznie zarządzanie za pośrednictwem stabilnych struktur polegające na podejmowaniu najważniejszych decyzji co do celów i sposobów przetwarzania. W motywie 36 wyjaśniono również, że „obecność i wykorzystywanie środków technicznych i technologii do przetwarzania danych osobowych lub do czynności przetwarzania nie stanowią same w sobie o głównej jednostce organizacyjnej, nie są więc kryteriami decydującymi o jej określeniu".

Administrator danych sam określa, gdzie znajduje się jego główna jednostka organizacyjna i w związku z tym – który organ nadzorczy jest jego wiodącym organem nadzorczym. Może to jednak zostać później zakwestionowane przez odpowiedni organ nadzorczy, którego sprawa dotyczy.

Poniższe czynniki są przydatne w celu ustalenia lokalizacji głównej jednostki organizacyjnej administratora zgodnie z warunkami określonymi w RODO w przypadkach, gdy nie jest to lokalizacja jego centralnej administracji w UE.

- Gdzie są ostatecznie zatwierdzane decyzje co do celów i sposobów przetwarzania?
- Gdzie są podejmowane decyzje dotyczące działalności gospodarczej obejmującej przetwarzanie danych?
- Komu przysługuje faktyczne uprawnienie do nakazania wykonania decyzji?
- Gdzie mieści się siedziba dyrektora (lub dyrektorów) obarczonych ogólnym obowiązkiem z zakresu zarządzania transgranicznym przetwarzaniem?

[2] W kontekście przetwarzania danych osobowych do celów bankowych uznaje się, że obejmuje ono wiele różnych czynności przetwarzania. W celu uproszczenia traktuje się jednak wszystkie z nich jako jeden cel. To samo dotyczy przetwarzania do celów ubezpieczeniowych.

[3] Należy również przypomnieć, że w RODO przewidziano możliwość nadzoru lokalnego w określonych przypadkach. Zob. motyw 127: „Każdy organ nadzorczy **niepełniący funkcji wiodącego** organu nadzorczego **powinien być właściwy w sprawach lokalnych**, gdy administrator lub podmiot przetwarzający posiadają jednostki organizacyjne w więcej niż jednym państwie członkowskim, ale przedmiot danego przetwarzania dotyczy **wyłącznie przetwarzania prowadzonego w pojedynczym państwie członkowskim i wyłącznie osób, których dane dotyczą, w tym pojedynczym państwie członkowskim**, na przykład gdy chodzi o przetwarzanie danych osobowych pracowników w szczególnym kontekście zatrudnienia w państwie członkowskim". Zasada ta oznacza, że kilka organów nadzorczych może być właściwych w zakresie sprawowania nadzoru nad danymi dotyczącymi zasobów ludzkich związanymi z kontekstem lokalnego zatrudnienia.

- Gdzie administrator lub podmiot przetwarzający są zarejestrowani jako przedsiębiorstwo, jeżeli są zarejestrowani na tym samym terytorium?

Należy zauważyć, że powyższy wykaz nie ma charakteru katalogu zamkniętego. Istotne mogą być inne czynniki, w zależności od danego administratora lub danej czynności przetwarzania. Jeżeli organ nadzorczy ma podstawy, by wątpić, czy dana jednostka organizacyjna ustalona przez administratora jest rzeczywiście główną jednostką organizacyjną do celów RODO, może – oczywiście – zwrócić się do administratora o podanie dodatkowych informacji niezbędnych do udowodnienia, gdzie znajduje się jego główna jednostka organizacyjna.

2.1.2 Grupy przedsiębiorstw

Jeżeli przetwarzania dokonuje grupa przedsiębiorstw, która ma siedzibę główną w UE, przyjmuje się, że jednostka administracyjna przedsiębiorstwa, która sprawuje całkowitą kontrolę, jest miejscem podejmowania decyzji dotyczących przetwarzania danych osobowych, i w związku z tym należy ją uznać za główną jednostkę organizacyjną grupy, z wyjątkiem sytuacji, gdy decyzje co do celów i sposobów przetwarzania są podejmowane przez inną jednostkę organizacyjną. Istnieje prawdopodobieństwo, że jednostka dominująca lub operacyjna siedziba główna grupy przedsiębiorstw w UE będzie główną jednostką organizacyjną, ponieważ jest to miejsce jej centralnej administracji.

Odniesienie w definicji do miejsca centralnej administracji administratora jest odpowiednie w przypadku organizacji, które mają scentralizowaną siedzibę główną podejmującą decyzje oraz strukturę obejmującą podział na oddziały. W takich przypadkach nie ulega wątpliwości, że uprawnienie do podejmowania decyzji dotyczących transgranicznego przetwarzania danych oraz do nakazania ich wykonania przysługuje siedzibie głównej przedsiębiorstwa. W tego rodzaju przypadkach ustalenie lokalizacji głównej jednostki organizacyjnej – i w związku z tym tego, który organ nadzorczy jest wiodącym organem nadzorczym – jest proste. System decyzyjny grupy przedsiębiorstw może być jednak bardziej złożony, obejmując nadanie uprawnienia do niezależnego podejmowania decyzji dotyczących transgranicznego przetwarzania różnym jednostkom organizacyjnym. Kryteria określone powyżej powinny pomóc grupom przedsiębiorstw w ustaleniu głównej jednostki organizacyjnej.

2.1.3 Współadministratorzy danych

W RODO nie uregulowano szczegółowo kwestii wyznaczania wiodącego organu nadzorczego wówczas, gdy co najmniej dwóch administratorów posiadających jednostki organizacyjne w UE wspólnie ustala cele i sposoby przetwarzania – tj. gdy są oni współadministratorami. W art. 26 ust. 1 i motywie 79 wyjaśniono, że w przypadku istnienia współadministratorów administratorzy w przejrzysty sposób określają odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z rozporządzenia. W celu skorzystania z zasady kompleksowej współpracy współadministratorzy powinni zatem wskazać, która jednostka organizacyjna współadministratorów (spośród jednostek administracyjnych, w których podejmowane są decyzje) będzie uprawniona do wykonania decyzji dotyczących przetwarzania w odniesieniu do wszystkich współadministratorów. Ta jednostka organizacyjna zostanie następnie uznana za główną jednostkę organizacyjną w zakresie przetwarzania dokonywanego w przypadku współadministratorów. Ustalenie dokonane przez współadministratorów pozostaje bez

uszczerbku dla zasad odpowiedzialności przewidzianych w RODO, w szczególności w art. 82 ust. 4.

2.2 Przypadki graniczne

Mogą zaistnieć sytuacje graniczne i złożone, w których trudno jest ustalić główną jednostkę organizacyjną lub określić, gdzie podejmowane są decyzje dotyczące przetwarzania danych. Może się to zdarzyć wówczas, gdy dokonywana jest czynność transgranicznego przetwarzania i administrator posiada jednostkę organizacyjną w kilku państwach członkowskich, ale nie ma centralnej administracji w UE, przy czym żadna z jednostek organizacyjnych w UE nie podejmuje decyzji dotyczących przetwarzania (tj. decyzje są podejmowane wyłącznie poza UE).

W powyższym przypadku przedsiębiorstwu dokonującemu transgranicznego przetwarzania może zależeć na podleganiu wiodącemu organowi nadzorczemu, aby mógł on skorzystać z zasady kompleksowej współpracy. W RODO nie przewidziano jednak rozwiązania tego rodzaju sytuacji. W tych okolicznościach przedsiębiorstwo jako główną jednostkę organizacyjną powinno wyznaczyć jednostkę organizacyjną, której przysługuje uprawnienie do wykonywania decyzji dotyczących czynności przetwarzania oraz do przyjęcia na siebie odpowiedzialności za przetwarzanie, w tym dysponującej wystarczającymi aktywami. Jeżeli przedsiębiorstwo nie wyznaczy głównej jednostki organizacyjnej w ten sposób, nie będzie możliwe wyznaczenie wiodącego organu nadzorczego. W stosownych przypadkach organy nadzorcze zawsze będą mogły bardziej dogłębnie zbadać sprawę.

W RODO nie dopuszcza się stosowania „turystyki sądowej". Jeżeli przedsiębiorstwo stwierdzi, że jego główna jednostka organizacyjna znajduje się w jednym z państw członkowskich, ale nie odbywa się w niej skuteczne i faktycznie zarządzanie ani nie podejmuje się w niej decyzji dotyczących przetwarzania danych osobowych, właściwy organ nadzorczy (lub ostatecznie Europejska Rada Ochrony Danych) zadecyduje o tym, który organ nadzorczy jest organem „wiodącym", stosując obiektywne kryteria i badając dowody. Proces ustalania, gdzie znajduje się główna jednostka organizacyjna, może wymagać szeroko zakrojonych czynności wyjaśniających i współpracy ze strony organów nadzorczych. Wnioski nie mogą się opierać jedynie na oświadczeniach organizacji poddawanej przeglądowi. Ciężar dowodu wykazania właściwym organom nadzorczym, gdzie podejmowane są istotne decyzje dotyczące przetwarzania danych oraz kto jest uprawniony do ich wykonania, spoczywa ostatecznie na administratorach i podmiotach przetwarzających. Rejestrowanie czynności przetwarzania danych pomogłoby w ustaleniu wiodącego organu nadzorczego zarówno organizacjom, jak i organom nadzorczym. Wiodący organ nadzorczy lub organy, których sprawa dotyczy, mogą podważyć analizę administratora w oparciu o obiektywne badanie istotnych faktów, wnioskując w stosownych przypadkach o dalsze informacje.

W niektórych przypadkach właściwe organy nadzorcze zwrócą się do administratora o przedstawienie jednoznacznych dowodów – zgodnie z wytycznymi Europejskiej Rady Ochrony Danych – potwierdzających, gdzie znajduje się jego główna jednostka organizacyjna lub gdzie podejmowane są decyzje dotyczące określonej czynności przetwarzania danych. Dowody te zostaną należycie uwzględnione, a zaangażowane organy nadzorcze będą współpracowały przy podejmowaniu decyzji dotyczących tego, który z nich będzie organem wiodącym w postępowaniach. Takie sprawy zostaną przekazane do rozpatrzenia Europejskiej Radzie Ochrony Danych na mocy artykułu 65 ust. 1 lit. b)

wyłącznie wówczas, gdy organy nadzorcze będą miały sprzeczne opinie w zakresie ustalenia wiodącego organu nadzorczego. W większości przypadków oczekuje się jednak, że właściwe organy nadzorcze będą w stanie uzgodnić wzajemnie satysfakcjonujący przebieg działania.

2.3 Podmiot przetwarzający

W RODO przewidziano również system kompleksowej współpracy korzystny dla przetwarzających, którzy podlegają RODO i posiadają jednostki organizacyjne w więcej niż jednym państwie członkowskim.

Artykuł 4 pkt 16 lit. b) RODO stanowi, że główną jednostką organizacyjną podmiotu przetwarzającego będzie miejsce, w którym znajduje się jego centralna administracja w UE, lub – wówczas, gdy podmiot przetwarzający nie ma centralnej administracji w UE – jednostka organizacyjna, w której odbywają się główne czynności przetwarzania (podmiotu przetwarzającego).

Zgodnie z motywem 36, jeżeli sprawa dotyczy zarówno administratora, jak i podmiotu przetwarzającego, właściwym wiodącym organem nadzorczym powinien być jednak wiodący organ nadzorczy administratora. W tej sytuacji organ nadzorczy podmiotu przetwarzającego zostanie „organem nadzorczym, którego sprawa dotyczy", i powinien on uczestniczyć w procedurze współpracy. Zasada ta będzie miała zastosowanie wyłącznie wówczas, gdy administrator posiada jednostkę organizacyjną w UE. W przypadkach, gdy administratorzy podlegają RODO na mocy art. 3 ust. 2, nie będą oni objęci mechanizmem kompleksowej współpracy. Podmiot przetwarzający może świadczyć usługi na rzecz wielu administratorów znajdujących się w różnych państwach członkowskich – na przykład na rzecz znaczącego dostawcy usług w chmurze. W takich przypadkach wiodącym organem nadzorczym będzie organ nadzorczy właściwy do podejmowania działań jako wiodący organ nadzorczy dla administratora. W rezultacie oznacza to, że istnieje możliwość, iż podmiot przetwarzający będzie musiał się kontaktować z wieloma organami nadzorczymi.

3. Inne istotne kwestie

3.1 Rola „organu nadzorczego, którego sprawa dotyczy"

Zgodnie z art. 4 pkt 22 RODO:

> „»organ nadzorczy, którego sprawa dotyczy« oznacza organ nadzorczy, którego dotyczy przetwarzanie danych osobowych, ponieważ: a) administrator lub podmiot przetwarzający posiadają jednostkę organizacyjną na terytorium państwa członkowskiego tego organu nadzorczego; b) przetwarzanie znacznie wpływa lub może znacznie wpłynąć na osoby, których dane dotyczą, mające miejsce zamieszkania w państwie członkowskim tego organu nadzorczego; lub c) wniesiono do niego skargę".

Pojęcie organu nadzorczego, którego sprawa dotyczy, ma zapewnić, by model „wiodącego organu nadzorczego" nie uniemożliwiał innym organom nadzorczym wyrażania opinii w zakresie sposobu rozpatrywania danej sprawy, na przykład wówczas, gdy czynność przetwarzania danych znacznie wpływa na osoby fizyczne zamieszkujące poza jurysdykcją organu wiodącego. Jeżeli chodzi o czynnik określony w lit. a) powyżej, zastosowanie mają te

same ustalenia co w przypadku ustalania wiodącego organu nadzorczego. Należy zauważyć, że w przypadku określonym w lit. b) osoba, której dane dotyczą, musi jedynie zamieszkiwać w danym państwie członkowskim; nie musi ona być obywatelem tego państwa. W przypadku określonym w lit. c) co do zasady łatwo będzie ustalić – jako okoliczność faktyczną – czy dany organ nadzorczy otrzymał skargę.

W art. 56 ust. 2 i 5 RODO przewidziano możliwość uczestnictwa w rozpatrywaniu sprawy przez organ nadzorczy, którego sprawa dotyczy, ale który nie jest jednak wiodącym organem nadzorczym. Jeżeli wiodący organ nadzorczy zdecyduje, że nie będzie rozpatrywał danej sprawy, sprawę tę rozpatruje organ nadzorczy, którego sprawa dotyczy i który przekazał informację wiodącemu organowi nadzorczemu. Jest to zgodne z procedurami określonymi w art. 61 (Wzajemna pomoc) oraz w art. 62 (Wspólne operacje organów nadzorczych) RODO. Może mieć to miejsce wówczas, gdy przedsiębiorstwo marketingowe posiadające główną jednostkę organizacyjną w Paryżu wprowadza do obrotu produkt, co wpływa jedynie na osoby, których dane dotyczą, zamieszkujące w Portugalii. W takim przypadku francuskie i portugalskie organy nadzorcze mogą uzgodnić, że właściwe jest przyjęcie wiodącej roli w rozpatrywaniu sprawy przez portugalski organ nadzorczy. Organy nadzorcze mogą zwrócić się do administratorów danych o wniesienie wkładu w postaci wyjaśnień dotyczących ich ustaleń korporacyjnych. Biorąc pod uwagę, że czynność przetwarzania ma wpływ czysto lokalny – tj. wywiera wpływ na osoby fizyczne w Portugalii – francuskim i portugalskim organom nadzorczym przysługuje swoboda uznania w zakresie decyzji, który organ nadzorczy powinien rozpatrzyć sprawę – zgodnie z motywem 127.

W RODO ustanowiono obowiązek współpracy wiodącego organu nadzorczego i organów nadzorczych, których sprawa dotyczy, przy należytym poszanowaniu wzajemnych poglądów, w celu zapewnienia, by sposób prowadzenia postępowania w sprawie i jej rozstrzygnięcie były satysfakcjonujące dla każdego z organów, przy jednoczesnym zapewnieniu prawa do skutecznego środka ochrony prawnej osobom, których dane dotyczą. Organy nadzorcze powinny dołożyć starań w celu osiągnięcia wzajemnie akceptowalnego przebiegu działania. Na oficjalny mechanizm spójności należy się powoływać wyłącznie wówczas, gdy współpraca nie przyniesie wzajemnie akceptowalnego rezultatu.

Wzajemna akceptacja decyzji może dotyczyć istotnych wniosków, ale również uzgodnionego przebiegu działania, w tym działań w zakresie egzekwowania (np. pełnego postępowania lub postępowania w ograniczonym zakresie). Może również dotyczyć decyzji o nierozpatrywaniu sprawy zgodnie z RODO, na przykład ze względu na oficjalną politykę ustanawiania priorytetów lub ze względu na istnienie innych organów, których sprawa dotyczy, jak opisano powyżej.

Wypracowanie konsensusu przez organy nadzorcze oraz ich dobra wola są niezbędne, by zapewnić sukces procesu współpracy i spójności zgodnie z RODO.

3.2 Lokalne przetwarzanie

Czynności lokalnego przetwarzania danych nie podlegają przepisom RODO dotyczącym współpracy i spójności. Organy nadzorcze będą szanować swoją wzajemną właściwość w zakresie rozpatrywania spraw dotyczących czynności lokalnego przetwarzania danych na szczeblu lokalnym. Sprawy dotyczące przetwarzania dokonywanego przez organy publiczne również zawsze będą rozpatrywane na szczeblu „lokalnym".

3.3 Przedsiębiorstwa nieposiadające jednostki organizacyjnej w UE

Mechanizm współpracy i spójności przewidziany w RODO ma zastosowanie wyłącznie do administratorów posiadających jednostkę organizacyjną lub jednostki organizacyjne w Unii Europejskiej. Jeżeli przedsiębiorstwo nie posiada jednostki organizacyjnej w UE, sama obecność przedstawiciela w państwie członkowskim nie powoduje uruchomienia systemu kompleksowej współpracy. Oznacza to, że administratorzy nieposiadający żadnej jednostki organizacyjnej w UE muszą się kontaktować z lokalnymi organami nadzorczymi w każdym państwie członkowskim, w którym działają, za pośrednictwem swoich lokalnych przedstawicieli.

Sporządzono w Brukseli dnia 13 grudnia 2016 r.

W imieniu Grupy Roboczej
Przewodnicząca
Isabelle FALQUE-PIERROTIN

Ostatnio zmienione i przyjęte w dniu 5 kwietnia 2017 r.

W imieniu Grupy Roboczej
Przewodnicząca
Isabelle FALQUE-PIERROTIN

ZAŁĄCZNIK – Pytania mające na celu pomoc w ustaleniu wiodącego organu nadzorczego

1. Czy administrator lub podmiot przetwarzający dokonuje transgranicznego przetwarzania danych osobowych?

a. Tak, jeżeli:

- administrator lub podmiot przetwarzający ma jednostkę organizacyjną w więcej niż jednym państwie członkowskim; oraz
- przetwarzanie danych osobowych odbywa się w ramach działalności jednostek organizacyjnych w więcej niż jednym państwie członkowskim.

➢ W tym przypadku należy przejść do pkt 2.

b. Tak, jeżeli:

- przetwarzanie danych osobowych odbywa się w ramach działności pojedynczej jednostki organizacyjnej administratora danych lub podmiotu przetwarzającego w Unii, ale:
- znacznie wpływa lub może znacznie wpłynąć na osoby fizyczne w więcej niż jednym państwie członkowskim.

➢ W tym przypadku wiodącym organem nadzorczym jest organ właściwy dla pojedynczej jednostki organizacyjnej administratora lub podmiotu przetwarzającego w pojedynczym państwie członkowskim. Logicznie rzecz biorąc, musi być to główna jednostka organizacyjna administratora lub podmiotu przetwarzającego, ponieważ jest to ich jedyna jednostka organizacyjna.

2. W jaki sposób można ustalić „wiodący organ nadzorczy"?

a. Jeżeli sprawa dotyczy wyłącznie administratora:

i. należy ustalić miejsce centralnej administracji administratora w UE;

ii. organ nadzorczy państwa, w którym znajduje się miejsce centralnej administracji, jest wiodącym organem nadzorczym właściwym dla administratora.

Należy jednak pamiętać, że:

iii. jeżeli decyzje co do celów i sposobów przetwarzania są podejmowane w innej jednostce organizacyjnej w UE, przy czym ta jednostka organizacyjna jest uprawniona do wykonania tych decyzji, wtedy wiodącym organem nadzorczym jest organ mający siedzibę w państwie, w którym znajduje się ta jednostka organizacyjna.

b. Jeżeli sprawa dotyczy administratora i podmiotu przetwarzającego:

i. należy sprawdzić, czy administrator posiada jednostkę organizacyjną w UE i czy podlega systemowi kompleksowej współpracy. Jeżeli tak,

ii. należy ustalić wiodący organ nadzorczy właściwy dla administratora. Organ ten będzie również wiodącym organem nadzorczym właściwym dla podmiotu przetwarzającego.

iii. Organ nadzorczy (niebędący wiodącym organem nadzorczym) właściwy dla podmiotu przetwarzającego będzie „organem, którego sprawa dotyczy" – zob. pkt 3 poniżej.

c. Jeżeli sprawa dotyczy wyłącznie podmiotu przetwarzającego:

i. należy ustalić miejsce centralnej administracji podmiotu przetwarzającego w UE;

(ii) jeżeli podmiot przetwarzający nie posiada centralnej administracji w UE, należy ustalić jednostkę organizacyjną w UE, w której odbywają się główne czynności przetwarzania prowadzone przez podmiot przetwarzający.

d. Jeżeli sprawa dotyczy współadministratorów:

(i) należy sprawdzić, czy współadministratorzy posiadają jednostki organizacyjne w UE;

(ii) należy wskazać – spośród jednostek administracyjnych, w których podejmowane są decyzje dotyczące celów i sposobów przetwarzania – jednostkę organizacyjną uprawnioną do wykonania tych decyzji w odniesieniu do wszystkich współadministratorów. Ta jednostka organizacyjna zostanie następnie uznana za główną jednostkę organizacyjną w zakresie przetwarzania dokonywanego przez współadministratorów. Wiodącym organem nadzorczym jest organ posiadający siedzibę w państwie, w której znajduje się ta jednostka organizacyjna.

3. Czy istnieją jakiekolwiek „organy nadzorcze, których sprawa dotyczy"?

Organ jest „organem, którego sprawa dotyczy":

- jeżeli administrator lub podmiot przetwarzający posiada jednostkę organizacyjną w jego jurysdykcji; lub
- jeżeli przetwarzanie znacznie wpływa lub może znacznie wpłynąć na osoby, których dane dotyczą, w jego jurysdykcji; lub
- w przypadku otrzymania skargi przez określony organ.

WP244 ZAŁĄCZNIK II – Często zadawane pytania

Czym jest wiodący organ nadzorczy?

Zgodnie z ogólnym rozporządzeniem o ochronie danych (RODO) co do zasady nadzór nad czynnością transgranicznego przetwarzania lub nad czynnością przetwarzania dotyczącą obywateli więcej niż jednego państwa UE sprawuje wyłącznie jeden organ nadzorczy zwany wiodącym organem nadzorczym. Określa się to mianem zasady kompleksowej współpracy.
Wiodący organ nadzorczy jest podmiotem, na którym spoczywa główna odpowiedzialność za prowadzenie postępowań dotyczących *czynności transgranicznego przetwarzania*, np. wówczas, gdy dane przedsiębiorstwo dokonuje czynności przetwarzania w kilku państwach członkowskich.

Wiodący organ nadzorczy skoordynuje działania dotyczące organów nadzorczych, których sprawa dotyczy, zgodnie z art. 60–62 rozporządzenia (np. mechanizm kompleksowej współpracy, wzajemną pomoc i wspólne operacje). Przedłoży wszelkie projekty decyzji organom nadzorczym posiadającym interes w danej sprawie.

Czym jest transgraniczne przetwarzanie?

Mechanizm wiodącego organu nadzorczego uruchamia się wyłącznie w kontekście transgranicznego przetwarzania. Konieczne jest zatem stwierdzenie, czy zachodzi przypadek transgranicznego przetwarzania.
Zgodnie z art. 4 pkt 23 rozporządzenia „transgraniczne przetwarzanie" oznacza:

- przetwarzanie danych osobowych, które odbywa się w Unii w ramach działalności jednostek organizacyjnych w więcej niż jednym państwie członkowskim administratora lub podmiotu przetwarzającego w Unii posiadającego jednostki organizacyjne w więcej niż jednym państwie członkowskim; albo

- przetwarzanie danych osobowych, które odbywa się w Unii w ramach działalności pojedynczej jednostki organizacyjnej administratora lub podmiotu przetwarzającego w Unii, ale które znacznie wpływa lub może znacznie wpłynąć na osoby, których dane dotyczą, w więcej niż jednym państwie członkowskim.

Co oznacza określenie „znacznie wpływać"?

W rozporządzeniu nie zdefiniowano określenia „znacznie wpływać".

Organy nadzorcze dokonają wykładni określenia „znacznie wpływa" w poszczególnych przypadkach. Należy uwzględnić kontekst przetwarzania, rodzaj danych, cel przetwarzania danych oraz czynniki, takie jak fakt, czy przetwarzanie:

- wyrządza lub może wyrządzić szkodę osobom fizycznym, naraża lub może je narazić na straty lub powoduje lub może spowodować stres u osób fizycznych;
- wywiera lub może wywierać faktyczne skutki w postaci ograniczenia praw lub pozbawienia możliwości;
- wpływa lub może wpływać na zdrowie, pomyślność lub spokój umysłu osób fizycznych;
- wpływa lub może wpływać na status finansowy lub gospodarczy osób fizycznych lub ich sytuację;

- naraża osoby fizyczne na dyskryminację lub niesprawiedliwe traktowanie;
- obejmuje analizę szczególnych kategorii danych osobowych lub innych danych wrażliwych, w szczególności danych osobowych dzieci;
- powoduje lub może spowodować znaczną zmianę zachowania osób fizycznych;
- ma mało prawdopodobne, nieoczekiwane lub niepożądane konsekwencje dla osób fizycznych;
- powoduje zakłopotanie lub ma inne negatywne skutki, w tym naruszenie dobrego imienia; lub
- obejmuje przetwarzanie szerokiego zakresu danych osobowych.

W jaki sposób można ustalić wiodący organ nadzorczy właściwy dla danego administratora?

Po ustaleniu, że dane przetwarzanie ma charakter transgraniczny, należy ustalić właściwy wiodący organ nadzorczy.

Zgodnie z art. 56 rozporządzenia właściwym wiodącym organem nadzorczym jest organ nadzorczy głównej jednostki organizacyjnej.

Jeżeli dana organizacja posiada pojedynczą jednostkę organizacyjną w UE, lecz przetwarzanie znacznie wpływa lub może znacznie wpłynąć na osoby, których dane dotyczą, w więcej niż jednym państwie członkowskim, właściwym wiodącym organem nadzorczym jest organ nadzorczy właściwy dla miejsca siedziby tej pojedynczej jednostki organizacyjnej.

Jeżeli dana organizacja ma kilka jednostek organizacyjnych w UE, co do zasady główną jednostką organizacyjną jest miejsce, w którym znajduje się centralna administracja tej organizacji. Jeżeli jednak inna jednostka organizacyjna decyduje o celach i sposobach przetwarzania – oraz przysługuje jej uprawnienie do nakazania wykonania takich decyzji – staje się ona główną jednostką organizacyjną. Obowiązek jednoznacznego ustalenia podmiotu odpowiedzialnego za podejmowanie decyzji co do celów i sposobów dokonywania czynności przetwarzania danych osobowych spoczywa na administratorach danych.

Przykładowo, jeżeli przedsiębiorstwo dokonuje jednej czynności transgranicznego przetwarzania lub kilku tego rodzaju czynności, przy czym decyzje dotyczące wszystkich czynności transgranicznego przetwarzania podejmowane są w położonym w UE miejscu, w którym znajduje się centralna administracja, jeden wiodący organ nadzorczy będzie właściwy w zakresie wszystkich czynności transgranicznego przetwarzania. Będzie to organ nadzorczy właściwy dla miejsca, w którym znajduje się centralna administracja przedsiębiorstwa.

Jeżeli jednak przedsiębiorstwo dokonuje kilku czynności transgranicznego przetwarzania, a decyzje co do sposobów i celów przetwarzania podejmowane są w różnych jednostkach organizacyjnych, właściwy będzie więcej niż jeden wiodący organ nadzorczy. Będą to organy właściwe dla miejsca, w którym znajdują się jednostki organizacyjne podejmujące decyzje dotyczące odpowiednich czynności transgranicznego przetwarzania. Aby w pełni korzystać z mechanizmu kompleksowej współpracy, w ramach którego jeden wiodący organ nadzorczy jest właściwy w zakresie wszystkich czynności transgranicznego przetwarzania, przedsiębiorstwa powinny rozważyć wprowadzenie rozwiązania, zgodnie z którym decyzje dotyczące czynności przetwarzania danych osobowych byłyby podejmowane w jednym miejscu.

Jakie kryteria stosuje się w celu ustalenia wiodącego organu nadzorczego właściwego dla danego administratora?

Poniższe czynniki mogą być przydatne przy ustalaniu położenia głównej jednostki organizacyjnej administratora:

- Czy jego pojedyncza jednostka organizacyjna znajduje się na terenie UE?

  Jeżeli tak oraz jeżeli przetwarzanie znacznie wpływa lub może znacznie wpłynąć na osoby, których dane dotyczą, w więcej niż jednym państwie członkowskim, właściwym wiodącym organem nadzorczym jest organ nadzorczy właściwy dla miejsca, w którym znajduje się ta pojedyncza jednostka organizacyjna.
- Czy jego siedziba główna znajduje się na terenie UE?

  - Jeżeli tak, jaką odgrywa rolę? Czy decyzje co do celów i sposobów przetwarzania podejmowane są w tej jednostce organizacyjnej? Oraz czy jednostce tej przysługuje uprawnienie do wykonywania decyzji dotyczących czynności przetwarzania?

  - Jeżeli nie, czy istnieją inne jednostki organizacyjne:

    - w których podejmowane są decyzje dotyczące działalności gospodarczej obejmującej przetwarzanie danych?
    - którym przysługuje faktyczne uprawnienie do nakazania wykonania decyzji?
    - w których mieści się siedziba dyrektora (lub dyrektorów) obarczonych ogólnym obowiązkiem z zakresu zarządzania czynnościami transgranicznego przetwarzania?
    - w których administrator lub podmiot przetwarzający są zarejestrowani jako przedsiębiorstwo, jeżeli są zarejestrowani na tym samym terytorium?

W jaki sposób można ustalić wiodący organ nadzorczy właściwy dla danego podmiotu przetwarzającego?

W rozporządzeniu do korzystania z systemu kompleksowej współpracy uprawniono również przetwarzających podlegających rozporządzeniu i posiadających jednostki organizacyjne w więcej niż jednym państwie członkowskim.

Art. 4 pkt 16 lit. b) stanowi, że główną jednostką organizacyjną podmiotu przetwarzającego będzie miejsce, w którym znajduje się jego centralna administracja w UE, lub – gdy podmiot przetwarzający nie ma centralnej administracji w UE – jednostka organizacyjna, w której odbywają się główne czynności przetwarzania (podmiotu przetwarzającego).

Zgodnie z motywem 36, jeżeli sprawa dotyczy zarówno administratora, jak i podmiotu przetwarzającego, właściwym wiodącym organem nadzorczym będzie jednak wiodący organ nadzorczy administratora. W tej sytuacji organ nadzorczy podmiotu przetwarzającego uznaje się za „organ nadzorczy, którego sprawa dotyczy", i powinien on uczestniczyć w procedurze współpracy.

ARTICLE 29 Data Protection Working Party

17/EN
WP264

Recommendation on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data

Adopted on 11 April 2018

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC. The secretariat is provided by Directorate C (Fundamental Rights and Union Citizenship) of the European Commission, Directorate General Justice, B-1049 Brussels, Belgium, Office No MO-59 02/013.
Website: http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358&tpa_id=6936

Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data[1]

Introduction and Instructions

The General Data Protection Regulation (EU) 2016/679 ('GDPR') allows personal data to be transferred outside the EEA only when the third country provides an "adequate level of protection" for the data (Art. 45) or when the controller adduces adequate safeguards with respect to the protection of privacy (Art. 46). Binding Corporate Rules (BCRs) are one of the ways in which such adequate safeguards (Art. 47) may be demonstrated by a group of undertakings, or group of enterprises engaged in a joint economic activity.

According to Article 64 GDPR, the use of BCRs as appropriate safeguards for international data transfers from the EEA requires the approval of the competent supervisory authority in accordance with the consistency mechanism set out in Article 63 without requiring any specific authorisation from a supervisory authority (Article 46.2.b GDPR). The following form is for use by companies seeking approval of BCRs. The form is based on papers previously issued by the Article 29 Working Party of European data protection authorities (the "Working Party"), and in particular WP133, and it is intended to help applicants demonstrate how to meet the requirements set out in Article 47 GDPR and WP 256.

General Instructions

- Only a single copy of the form need be filled out and submitted to the Supervisory Authority ('SA') you consider to be the lead authority for the BCRs ('BCR lead') in accordance with Article 47.1 and 64 GDPR and WP 263; this form may be used in all EEA Member States.
- Please fill out all entries and submit the form to the SA you consider to be the BCR lead.
- You may attach additional pages or annexes if there is insufficient space to complete your responses.
- You may indicate any responses or materials that is in your opinion commercially sensitive and should be kept confidential but, in any case, be aware that the relevant document will be shared among the concerned SAs and the European Data Protection Board (EDPB) which, under Article 64, has to issue its opinion on the approval draft decision of your BCRs. Requests by third parties for disclosure of such information, will, however, be handled by each supervisory authority involved in accordance with national legislation.
- The footnotes in the application form indicate the relevant provisions of the Article 47 GDPR and Working Party papers WP 256 and specific Sections of WP 74 and WP 108, which contain further clarification of the questions still valid under the framework of the GDPR.
- Once you have submitted the form, the SA you approached will circulate Part 1 of the form to all the 'concerned supervisory authorities'[2] in order to determine who should be the BCR Lead;

[1] This questionnaire takes also into account the draft standard application form for approval of Binding Corporate Rules drawn up by the ICC.
[2] Pursuant to Article 4(22)(a) and (b), a 'supervisory authority concerned' means a supervisory authority which is concerned by the processing of personal data because the controller or processor is established on the territory of

- You will be informed by the SA you approached which SA has finally been appointed by all SAs concerned to act as BCR Lead;
- As a rule, the BCR Lead will seek the cooperation of two other SAs concerned (SAs co-reviewers) in order to assess the BCRs in the light of Article 47 and WP 256[3];
- Once revised, in accordance with Article 64 GDPR, the BCR Lead will circulate the remainder of the form including your BCRs to all the other supervisory authorities concerned in order to collect their views to be sent to European Data Protection Board (EDPB) along with the draft opinion on the BCRs.

PART 1 APPLICANT INFORMATION

Section 1: Structure and Contact Details of the Applicant and of the Group of group of undertakings, or group of enterprises engaged in a joint economic activity ('Group')

- If the Group has its headquarters in the EEA the form should be filled out and submitted by that EEA entity.
- If the Group has its headquarters outside the EEA, then the Group should appoint a Group entity located inside the EEA – preferably established in the country of the presumptive BCR Lead - as the Group member with "delegated data protection responsibilities". This is the entity which should then submit the application on behalf of the Group.
- Contact Details of the Responsible Party for Queries:
    - Please indicate a responsible party to whom queries may be addressed concerning the application.
    - This party need not be located in the EEA, although this might be advisable for practical reasons.
    - You may indicate a function rather than a specific person.

Section 2: Short description of data flows

- The applicant should also give a brief description of the scope and nature of the data flows from the EEA for which approval is sought.

Section 3: Determination of the BCRs Lead

- In accordance with Article 64 GDPR, the BCR Lead is the authority in charge of coordinating the approval of your BCRs which then could be considered to be appropriate safeguards in the countries within the EEA which you have named in your application as the origin of transfers of personal data by Group members to third countries, without requiring any specific authorisation for the use of the BCR from the other supervisory authorities concerned.
    - Before you approach one SA as the presumptive BCR Lead you should examine the factors listed in Section 1of WP 263 (still the same already enlisted in Sections 3.3 and 3.4. of WP 108). Based on these factors you should explain in Part 1.3 of your application which SA should be the BCR Lead. The SAs are not obligated to accept the choice that you make if they believe that another SA is more suitable to be BCR Lead, in particular if it would be worth for speeding up the procedure (e.g. taking into account the workload of the originally requested SA).

PART 2 BACKGROUND PAPER

Section 4: Binding Nature of the Binding Corporate Rules

- In order for the BCRs to be approved for the transfer of personal data, they must be shown to have legally binding effect both internally (between the Group entities, and on employees and subcontractors) and externally (for the benefit of individuals whose personal data is processed by the Group) in accordance with national legislation. These questions elicit the information necessary to determine if your BCRs have such binding effect.
- Your application will need to make clear that the burden of proof with regard to an alleged breach of the rules will rest with one member of the Group established on the territory of a Member State (e.g. the member at the origin of the transfer or the European headquarters

the Member State of that supervisory authority or because "data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing". As for the BCRs approval procedure, the concerned SAs are the SAs in the countries from where the transfers are to take place as specified by the applicants or, in case of BCR-P, all SAs (since a processor established in a Member State may provide services to controllers in several – potentially all – Member States).

[3] As a rule, the BCR Lead will consult 2 co-reviewers whenever 14 Member States are concerned by transfers. Under this threshold it is possible to have one or two co-reviewers depending on the specific case and the availability of SAs.

or that part of the organisation with delegated data protection responsibilities), regardless of where the claim originates.

- Regulators in some sectors (such as the financial services industry) may prohibit an entity of the Group in one country from assuming liability for another Group entity in another country. If this is the case for your application, please provide details about this situation in the subsection "Legal claims or actions" and explain any other mechanisms your Group has implemented to ensure that an aggrieved individual can obtain recourse against the Group in the EEA.

Section 5: Effectiveness

- Effectiveness (verification of compliance) may be demonstrated by a variety of mechanisms typically implemented by companies, such as a regular audit programme, corporate governance activities, compliance departments, etc. Please respond to the questions on effectiveness based on the verification mechanisms used in your group.
- You will need to confirm that you will permit the concerned SAs in the EEA to audit your compliance.

Section 6: Cooperation with SAs

- Section 6 focuses on cooperation with SAs. You have to specify how your BCRs deal with the cooperation with SAs.

Section 7: Description of Processing and Data Flows

- In order for the SAs to assess whether your BCRs provide adequate safeguards for the transfers of data in accordance with Article 47 GDPR, it is essential that you describe data flows within your Group in a complete yet understandable fashion.

Section 8: Mechanisms for Reporting and Recording Changes

- Both the SAs and the Group entities must be informed without undue delay about any changes to the BCRs. In particular, changes that significantly affect data protection compliance (e.g. will be detrimental to data subject rights), and not to mere administrative changes (unless they impact the BCRs - e.g. changes to the bindingness) must be promptly communicated to the concerned Supervisory Authorities, via the competent SA under Article 64 (i.e. BCR Lead)[4]. In this section, please describe the mechanisms your Group has implemented for reporting and recording such changes.
- The obligation to report changes applies only to the text of the BCRs themselves, and not to any supporting documentation, unless a change to such documentation would significantly affect compliance with the BCRs.

Section 9: Data Protection Safeguards

- In this Section please provide details of how your BCRs address the core data protection safeguards that are necessary to provide an adequate level of protection for the data that are transferred.

Annex 1: Copy of the Formal Binding Corporate Rules

- Please attach a copy of your BCRs. These need not necessarily be contained within one document and your BCRs may comprise a number of documents. In the latter case please clearly specify the legal relationship between these documents (e.g. general rules – more detailed rules for a specific area like HRM or CRM).

[4] See WP 155, Q 14.

- You do not need to attach all ancillary documentation at this stage, this may be submitted separately after discussions with the BCR Lead.

Standard Application for Approval of Binding Corporate Rules

PART 1: APPLICANT INFORMATION

1. STRUCTURE AND CONTACT DETAILS OF THE GROUP OF UNDERTAKINGS OR GROUP OF ENTERPRISES ENGAGED IN A JOINT ECONOMIC ACTIVITY (THE GROUP)
Name of the Group and location of its headquarters:
Does the Group have its headquarters in the EEA? ☐ Yes ☐ No

Name and location of the applicant:		
Identification number (if any):		
Legal nature of the applicant (corporation, partnership, etc.):		
Description of position of the applicant within the Group: (e.g. headquarters of the Group in the EEA, or, if the Group does not have its headquarters in the EEA, the member of the Group inside the EEA with delegated data protection responsibilities)		
Name and/or function of contact person (note: the contact person may change, you may indicate a function rather than the name of a specific person):		
Address:		
Country:		
Phone number:	Fax:	E-Mail:

EEA Member States from which BCRs will be used:

2. SHORT DESCRIPTION OF PROCESSING AND DATA FLOWS[5]
Please, indicate the following: - Nature of the data covered by BCRs, and in particular, if they apply to one category of data or to more than one category, the type of processing and its purposes, the types of data subjects affected ((for instance data related to employees, customers, suppliers and other third parties as part of its respective regular business activities,…) - Do the BCRs only apply to transfers from the EEA, or do they apply to all transfers between members of the group? - Please specify from which country most of the data are transferred outside the EEA: - Extent of the transfers within the Group that are covered by the BCRs; including a description and the contact details of any Group members in the EEA or outside EEA to which personal data may be transferred

3. DETERMINATION OF THE LEAD SUPERVISORY AUTHORITY ('BCR LEAD')[6]
Please explain which should be the BCR Lead, based on the following criteria: - Location of the Group's EEA Headquarters - If the Group is not headquartered in the EEA, the location in the EEA of the Group entity with delegated data protection responsibilities - The location of the company which is best placed (in terms of management function, administrative burden, etc.) to deal with the application and to enforce the binding corporate rules in the Group - Country where most of the decisions in terms of the purposes and the means of the data processing are taken - EEA Member States from which most of the transfers outside the EEA will take place

[5] See Article 47.2. a and b and Section 4.1. WP 256.
[6] See Part. 1 WP 263.

PART 2: BACKGROUND PAPER[7]

4. BINDING NATURE OF THE BINDING CORPORATE RULES (BCRs)

INTERNAL BINDING NATURE[8]

Binding within the entities of the Group[9]

How are the BCRs made binding upon the members of the Group?

- ☐ Measures or rules that are legally binding on all members of the Group
- ☐ Contracts or intra-group agreement between the members of the Group
- ☐ Unilateral declarations or undertakings made or given by the parent company which are binding on the other members of the Group (this is only possible if the BCR member taking responsibility and liability is located in a Member State that recognizes Unilateral undertakings as binding and if this BCR member is legally able to bind the other members subject to BCRs)
- ☐ Other means (only if the group demonstrates how the binding character of the BCRs is achieved), please specify

Please explain how the mechanisms you indicated above are legally binding on the members of the Group in the sense that they can be enforced by other members of the Group (esp. headquarters):

Does the internally binding effect of your BCRs extend to the whole Group? (If some Group members should be exempted, specify how and why)

[7] Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, WP 256, adopted on 6 February 2018.
[8] See GDPR Art. 47.1.a and 47.2.c and Section 1.2 WP 256. See, also, general considerations in Section 3.3.1. WP74 and in Section 5 WP108.
[9] See Section 5.3 WP108.

Binding upon the employees[10]

Your Group may take some or all of the following steps to ensure that the BCRs are binding on employees, but there may be other steps. Please, give details below.

- Work employment contract

- Collective agreements (approved by workers committee/another body)

- Employees must sign or attest to have read the BCRs or related ethics guidelines in which the BCRs are incorporated

- BCRs have been incorporated in relevant company policies

- Other means (but the group must properly explain how the BCRs are made binding on employees)

- Disciplinary sanctions for failing to comply with relevant company policies, including dismissal for violation

Please provide a summary supported by extracts from policies and procedures or confidentiality agreements as appropriate to explain how the BCRs are binding upon employees.

Binding upon subcontractors processing the data[11]

What steps have you taken to require subcontractors to apply protections to the processing of personal data (e.g., through the use of obligations in your contracts with them)? Please specify:

How do such contracts or other legal acts under Union or Member State law address the consequences of non-compliance?

Please specify the sanctions imposed on subcontractors for failure to comply

[10] See Article 47.1.a and Section 1.2 WP 256 and Section 5.8 WP108.
[11] See Art. 28.3 GDPR and Section 5.10 WP108.

EXTERNALLY BINDING NATURE[12]

How are the rules binding externally for the benefit of individuals (third party beneficiary rights) or how do you intend to create such rights? For example you might have created some third party beneficiary rights in contracts or unilateral declarations[13].

Legal claim or actions
Explain how you meet the obligations according to the requirement of Articles 47.2.e, 77 and 79, 82 GDPR[14]

Please confirm that the controller established on the territory of a Member State (e.g. the European headquarters of the Group, or that part of the Group with delegated data protection responsibilities in the EEA), has made appropriate arrangements to enable itself or the member of the Group at the origin of the transfer payment of compensation for any damages resulting from the breach, by any part of the Group, of the BCRs and explain how this is ensured.
Please confirm that the burden of proof with regard to an alleged breach of the rules will rest with the member of the Group at the origin of the transfer or the European headquarters or that part of the organisation in the EEA with delegated data protection responsibilities, regardless of where the claim originates.

[12] See 47.1.b and 47.2.c and e GDPR and Section 1.3 WP 256. See also general considerations in Section 3.3.2 WP74.

[13] Data subjects must at least be able to enforce the following elements of the BCRs:

- Data protection principles (Art. 47.2.d and Section 6.1 WP 256),
- Transparency and easy access to BCRs (Art. 47.2.g and Section 6.1, Section 1.7 WP 256),
- Rights of access, rectification, erasure, restriction, objection to processing, right not to be subject to decisions based solely on automated processing, including profiling (GDPR Art. 47.2.e and Art. 15, 16, 17,18, 21, 22),
- National legislation preventing respect of BCRs (Art. 47.2.m and Section 6.3 of this referential),
- Right to complain through the internal complaint mechanism of the companies (Art. 47.1.i and Section 2.2 WP 256),
- Cooperation duties with Data Protection Authority (Art. 47.2.k and l, Section 3.1 WP 256),
- Liability and jurisdiction provisions (Art. 47.2.e and f, Section 1.3, 1.4 WP 256).

Furthermore, you must be fully aware of the fact that according to civil law of some jurisdictions unilateral declarations or unilateral undertakings do not have a binding effect. In the lack of a specific legislative provision on bindingness of such declarations, only a contract with third party beneficiary clauses between the members of the Group may give proof of bindingness.

[14] See also Section 1.3. WP 256: the BCRs must confer the right to lodge a complaint with the competent supervisory authority (choice before the SA in the Member State of his habitual residence, place of work or place of the alleged infringement, pursuant to art. 77 GDPR) and before the competent court of the EU Member States (choice for the data subject to act before the courts where the controller or processor has an establishment or where the data subject has his or her habitual residence pursuant to Article 79 GDPR).

5. EFFECTIVENESS[15]

It is important to show how the BCRs in place within your organization are brought to life in practise, in particular in non EEA countries where data will be transferred on the basis of the BCRs, as this will be significant in assessing the adequacy of the safeguards.

Training and awareness raising (employees)
- Special training programs - Employees are tested on BCRs and data protection - BCRs are communicated to all employees on paper or online - Review and approval by senior officers of the company - How are employees trained to identify the data protection implications of their work, i.e. to identify that the relevant privacy policies are applicable to their activities and to react accordingly? (This applies whether these employees are or not based in the EEA)

Internal complaint handling[16]
Do the BCRs contain an internal complaint handling system to enforce compliance? Please describe the system for handling complaints:

[15] See Articles 47.2.j and 47.2.l and Art. 38.3 GDPR and Section 2.3 WP 256. See also general considerations in Section 5.2 WP74 and Section 6 WP108.

[16] See Articles 47.2.i and 12.3 GDPR and Section 2.2 WP 256. See also Section 5.3 WP74.

Verification of compliance

What verification mechanisms does your Group have in place to audit each member's compliance with your BCRs? (e.g., an audit programme, compliance programme, etc)? Please specify:

Please explain how your verification or compliance programme functions within the Group (e.g., information as to the recipients of any audit reports and their position within the structure of the Group).

Do the BCRs provide for the use of:

- Data Protection Officer? Choose by clicking here
- internal auditors? Choose by clicking here
- external auditors? Choose by clicking here
- a combination of both internal and external auditors? Choose by clicking here
- verification by an internal compliance department? Choose by clicking here

Do your BCRs mention if the verification mechanisms are clearly set out in…

- a document containing your data protection standards Choose by clicking here
- other internal procedure documents and audits? Choose by clicking here

Network of data protection officers (DPO) or appropriate staff[17]

Please confirm that a network of DPOs or appropriate staff (such as a network of privacy officers) is appointed with top management support to oversee and ensure compliance with the BCR for Processors:

Please explain how your network of DPOs or privacy officers functions:

- Internal structure:

- Role and responsibilities:

6. COOPERATION WITH SAs[18]

Please, specify how your BCRs deal with the issues of cooperation with SAs:

Do you confirm that you will permit the concerned SAs to audit your compliance?

Do you confirm that the Group as a whole and each of the companies of the Group will abide by the advice of the concerned Supervisory authority relating to the interpretation and the application of your BCRs?

[17] See Section 2.4 WP 256.
[18] See Article 47.2.l GDPR and Section 3.1 WP 256 and Section 5.4 WP 74.

7. DESCRIPTION OF PROCESSING AND DATA FLOWS[19]

Please indicate the following:

- Nature of the data covered by the BCRs, e.g. HR data, and in particular, if they apply to one category of data or to more than one category

- What is the nature of the personal data being transferred?

- In broad terms where do the data flow to and from?

- What are the type of processing and the purposes for which the data covered by the BCRs are transferred to third countries and of the processing that is carried out after the transfers?

- Extent of the transfers within the Group that are covered by the BCRs, including a description and contact details of any Group members in the EEA or outside the EEA to which personal data may be transferred

Do the BCRs only apply to transfers from the EEA, or do they apply to all transfers between members of the Group? Please specify:

[19] See Article 47.2.b GDPR and Section 4.1 WP 256 and Section 7 WP108.

8. MECHANISMS FOR REPORTING AND RECORDING CHANGES[20]

Please, confirm and explain how your BCRs allow for informing other parts of the Group and the concerned SAs, via the competent SA under Article 64 (i.e. the BCR Lead), of any changes to the BCRs and/or the list of BCR members (summary):

Please confirm that you have put in place a system to record any changes to your BCRs.

9. DATA PROTECTION SAFEGUARDS[21]

Please, specify with reference to your BCRs how and where the following issues are addressed with supporting documentation where appropriate:

- Transparency and fairness and lawfulness

- Purpose limitation

- Data minimisation and accuracy

- Limited storage periods

- Processing of special categories of personal data

- Security (including the obligation to enter into contracts with all internal and external subcontractors/processors which comprise all requirements as set out in Art. 28.3 GDPR and as well the duty to notify without undue delay any personal data breaches to the EU headquarters or the EU BCR member with delegated data protection responsibilities and the other relevant Privacy Officer/Function and data subjects where the personal data breach is likely to result in a high risk to their rights and freedoms)

- Restrictions on onward transfers

- Other (e.g. protection of children, etc.)

[20] See Article 47.2.k GDPR and Section 5.1. WP 256.
[21] See Article 47.2.d GDPR and Section 6.1. WP 256.

10. ACCOUNTABILITY AND OTHER TOOLS[22]
-Please confirm and specify how BCR members will be responsible for and able to demonstrate compliance with the BCRs -Please confirm that the BCR members will maintain a record of all categories of processing activities carried out on behalf of each controller in line with the requirements as set out in Art. 30.1 GDPR. -Please confirm that data protection impact assessments will be carried out for processing operations that are likely to result in a high risk to the rights and freedoms of natural persons (GDPR Art. 35) and that where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk, the competent supervisory authority, prior to processing, should be consulted (GDPR Art. 36) - Please confirm and specify which appropriate technical and organisational measures will be implemented to comply with data protection principles and facilitate compliance with the requirements set up by the BCRs in practice (e.g. data protection by design and by default, GDPR Art. 25) Please provide supporting documents where appropriate with respect to the information requested above

[22] See Section 6.1.2 WP256

ANNEX 1:
COPY OF THE FORMAL BINDING CORPORATE RULES

Please attach a copy of your BCRs. Note that this does not include any ancillary documentation that you would like to submit (e.g. specific privacy policies and rules).

ARTICLE 29 DATA PROTECTION WORKING PARTY

17/EN
WP265

Recommendation on the Standard Application form for Approval of Processor Binding Corporate Rules for the Transfer of Personal Data

Adopted on 11 April 2018

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC. The secretariat is provided by Directorate C (Fundamental Rights and Union Citizenship) of the European Commission, Directorate General Justice, B-1049 Brussels, Belgium, Office No MO-59 02/013.
Website: http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358&tpa_id=6936

Standard Application for Approval of Binding Corporate Rules for Processors

PART 1: APPLICANT INFORMATION

1. STRUCTURE AND CONTACT DETAILS OF THE GROUP OF UNDERTAKINGS OR GROUP OF ENTERPRISES ENGAGED IN A JOINT ECONOMIC ACTIVITY (THE GROUP)

Name of the Group and location of its headquarters (ultimate parent company):
Does the Group have its headquarters in the EEA? ☐ Yes ☐ No

Name and location of the applicant:		
Identification number (if any):		
Legal nature of the applicant (corporation, partnership, etc.):		
Description of position of the applicant within the Group: (e.g. headquarters of the Group in the EEA, or, if the Group does not have its headquarters in the EEA, the member of the Group inside the EEA with delegated data protection responsibilities)		
Name and/or function of contact person (note: the contact person may change, you may indicate a function rather than the name of a specific person):		
Address:		
Country:		
Phone number:	Fax:	E-Mail:

EEA Member States from which BCRs for Processors will be used:

2. SHORT DESCRIPTION OF PROCESSING AND DATA FLOWS

Please, indicate the following:

- Expected nature of the data covered by BCR, and in particular, if they apply to one category of data or to more than one category, types of data subjects concerned, (for instance human resources, customers,…), anticipated types of processing and its purposes

- Anticipated purposes of data transfers for processing activities

- Do the BCR only apply to transfers from the EEA, or do they apply to all transfers for processing activities between members of the Group?

- Please specify from which country most of the data are transferred outside the EEA for processing activities:

- Extent of the transfers within the Group that are covered by the BCR; including a description and contact details of any Group members in the EEA or outside EEA to which personal data may be transferred for processing activities

3. DETERMINATION OF THE LEAD SUPERVISORY AUTHORITY (BCR LEAD)

Please explain which should be the BCR Lead, based on the following criteria:

- Location of the Group's EEA headquarters

- If the Group is not headquartered in the EEA, the location in the EEA of the Group entity with delegated data protection responsibilities

- The location of the company which is best placed (in terms of management function, administrative burden, etc.) to deal with the application and to enforce the binding corporate rules in the Group

- EEA Member States from which most of the transfers outside the EEA will take place

PART 2: BACKGROUND PAPER[1]

4. BINDING NATURE OF THE BINDING CORPORATE RULES (BCR) FOR PROCESSORS

INTERNAL BINDING NATURE[2]

Binding within the entities of the Group acting as internal subprocessors[3]

How are the BCR for processors made binding upon the members of the Group?

- ☐ Measures or rules that are legally binding on all members of the Group
- ☐ Contracts or intra-group agreements between the members of the Group
- ☐ Unilateral declarations or undertakings made or given by the parent company which are binding on the other members of the Group (that is only possible if the BCR member taking responsibility and liability is located in a Member State that recognizes Unilateral declarations or undertakings as binding and if this BCR member is legally able to bind the other members subject to BCRs);
- ☐ Other means (only if the Group demonstrates how the binding character of the BCRs is achieved), please specify

Please explain how the mechanisms you indicated above are legally binding on the members of the Group in the sense that they can be enforced by other members of the Group (esp. headquarters):

Does the internally binding effect of your BCR for Processors extend to the whole Group? (If some Group members should be exempted, specify how and why)

Please confirm that any use of subprocessors (internal) is only done after prior information to data controllers and with their prior written consent

[1] Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, WP257, adopted on 6 February 2018.
[2] See Section 1.1 and 1.2 WP 257
[3] See Section 1.2 (i) WP 257

Binding upon the employees[4]
Your Group may take some or all of the following steps to ensure that the BCR for Processors are binding on employees, but there may be other steps. Please, give details below. -Individual and separate agreement/undertaking with sanctions - Work employment contract with sanctions - Collective agreements (approved by workers committee/another body) with sanctions - Employees must sign or attest to have read the BCR for Processors or related ethics guidelines in which the BCR for Processors are incorporated - BCR for Processors have been incorporated in relevant company policies with sanctions - Disciplinary sanctions for failing to comply with relevant company policies, including dismissal for violation - Other means (but the group must properly explain how the BCRs are made binding on employees) Please provide a summary supported by extracts from policies and procedures or confidentiality agreements as appropriate to explain how the BCR for Processors are binding upon employees.

[4] See Section 1.2 (ii) WP257

EXTERNALLY BINDING NATURE

Binding upon external subprocessors processing the data
Please confirm that a written contract or other legal act under Union or Member State law is put in place with external subprocessors which states that adequate protection is provided according to Articles 28, 29, 32, 45, 46, 47 of the GDPR and which ensures that the external subprocessors will have to respect the same data protection obligations as are imposed on the Group members according to the Service Agreements concluded with data controllers and Sections 1.3, 1.4, 3 and 6 of WP257[5].
How do such contracts or other legal acts under Union or Member State law address the consequences of non compliance? Please specify the sanctions imposed on subprocessors for failure to comply
Please confirm that any use of subprocessors (external) is only done after prior informed specific or general written authorization of the data controller[6]
Please confirm that subprocessors accept to submit their data processing facilities for audit, at the request of a data controller, of the processing activities relating to that controller[7]. Please describe the system.

How are the rules binding externally for the benefit of individuals (third party beneficiary rights) or how do you intend to create such rights? For example you might have created some third party beneficiary rights in contracts or unilateral declarations[8].
Please provide a summary supported by extracts from the agreement signed with data controllers as appropriate to explain how the BCR for Processors are made binding towards data controllers[9] Please confirm that data controllers' rights shall cover the judicial remedies and the right to receive compensation

[5] See Section 6.1 (vii) WP257
[6] See Section 6.1 (vii) WP257
[7] See Section 2.3 WP 257
[8] You must be fully aware of the fact that according to civil law of some jurisdictions (e.g. Italy or Spain) unilateral declarations or unilateral undertakings do not have a binding effect. In the absence of a specific legislative provision on bindingness of such declarations, only a contract with third party beneficiary clauses between the members of the Group may give proof of bindingness.
[9] See Section 1.4 WP 257

Legal claim or actions
Explain how you meet the obligations according to the requirements of Article 47.2.e, 77, 79, 82, as further specified in paragraph 1.3 of WP257[10]

Please confirm that the controller established on the territory of a Member State (e.g. EEA headquarters of the Group, the Group member of the Processor with delegated data protection responsibilities in the EEA or the EEA exporter processor (e.g., the EEA contracting party with the controller), has made appropriate arrangements to enable itself to remedy the acts and to pay compensation, for any damages suffered either by a data subject or a data controller, resulting from the breach, by any member of the Group or by any external subprocessor, of the BCR for Processors and explain how this is ensured.
Please confirm that the burden of proof with regard to an alleged breach of the rules caused either by a Group member or by an external subprocessor will rest with the member of the Group in the EU that have accepted to endorse liability for breaches caused by non EEA members of the group or by subprocessors, regardless of where the claim originates.

Easy access to BCR for Processors[11]

Please confirm that your BCR for Processors are annexed to the Service Agreements signed with data controllers, or that reference to it is made with a possibility of electronic access:
Please confirm that your BCR for Processors are published on the website of the Group of processor in a way easily accessible to data subjects, or at least that a document is published and contains all the information as required in Section 1.8 of WP257:

[10] 1.3 WP 257 provides that the BCRs must grant rights to data subjects to enforce BCRs as third party beneficiaries against the processor either when the requirements at stake are specifically directed to processors in accordance with the GDPR or in case the data subject is not able to bring a claim against the data controller because the data controller has factually disappeared or ceased to exist in law or has become insolvent, unless any successor entity has assumed the entire legal obligations of the data controller by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

[11] See Section 1.8 WP257

5. EFFECTIVENESS[12]

It is important to show how the BCR for Processors in place within your Group are brought to life in practice, in particular in non EEA countries where data will be transferred for processing activities on the basis of the BCR for Processors, as this will be significant in assessing the adequacy of the safeguards.

Training and awareness raising (employees)[13]

- Special training programs - Employees are tested on BCR for Processors and data protection - BCR for Processors are communicated to all employees on paper or online - Review and approval by senior officers of the company - How are employees trained to identify the data protection implications of their work, i.e. to identify that the relevant privacy policies are applicable to their activities and to react accordingly? (This applies whether these employees are or not based in the EEA)

Internal complaint handling[14]

Do the BCR for Processors contain an internal complaint handling system to (i) communicate claims or requests without delay to data controllers, and to (ii) handle complaints instead of a data controller when the latter has disappeared factually, has ceased to exist in law or became insolvent, or when it has been agreed with a data controller that the Group will handle claims and requests from data subjects? Please describe the system for handling complaints:

[12] See Section 2 WP257

13 See Section 2.1 WP257

[14] See Section 2.2 WP257

***Verification of compliance*[15]**

What verification mechanisms do your Group have in place to audit each Group members' compliance with your BCR for Processors? (e.g., an audit programme, compliance programme, etc)? Please specify:

Please explain how your verification or compliance programme functions within the Group (e.g., information as to the recipients of any audit reports and their position within the structure of the Group).

Do the BCR for Processors provide for the use of:

- Data Protection Officer?	Choose by clicking here
- internal auditors?	Choose by clicking here
- external auditors?	Choose by clicking here
- a combination of both internal and external auditors?	Choose by clicking here
- verification by an internal compliance department?	Choose by clicking here

Do your BCR for Processors mention if the verification mechanisms are clearly set out in…

- a document containing your data protection standards	Choose by clicking here
- other internal procedure documents and audits?	Choose by clicking here

***Network of data protection officers (DPO) or appropriate staff*[16]**

Please confirm that a network of DPOs or appropriate staff (such as a network of privacy officers) is appointed with top management support to oversee and ensure compliance with the BCR for Processors:

Please explain how your network of DPOs or privacy officers functions:

- Internal structure:

- Role and responsibilities:

[15] See Section 2.3 WP 257
[16] See Section 2.4 WP 257

6. COOPERATION WITH SAs[17]

Please, specify how your BCR for Processors deal with the issues of cooperation with SAs:

Do you confirm that you will permit the relevant SAs to audit your compliance?

Do you confirm that the Group as a whole and each members of the Group will abide by the advice of the relevant Supervisory authorities relating to the interpretation and the application of your BCR for Processors?

7. COOPERATION WITH DATA CONTROLLERS[18]

Please specify how your BCR for Processors deal with the duty of cooperation with data controllers?

Do you confirm that you will submit your data processing facilities to data controller (or to an inspection body composed of independent members, selected by the data controller) which requested it for audits of the processing activities relating to them?

[17] See Section 3.1 WP257
[18] See Section 3.2 WP 257

8. DESCRIPTION OF PROCESSING AND DATA FLOWS[19]

Please indicate the following:

- Expected nature of the data covered by the BCR for Processors, e.g. HR data, and in particular, if they apply to one category of data or to more than one category

- What is the nature of the personal data being transferred for processing activities?

- In broad terms what is the extent of the flow of data?

- Purposes for which the data covered by the BCR for Processors are transferred to third countries and type of processing

- Extent of the transfers within the Group that are covered by the BCR for Processors, including a description and contact details of any Group members in the EEA or outside the EEA to which personal data may be transferred for processing activities

Do the BCR only apply to transfers for processing activities from the EEA, or do they apply to all transfers for processing activities between members of the Group? Please specify:

8. MECHANISMS FOR REPORTING AND RECORDING CHANGES[20]

[19] See Section 4.1 WP257

[20] See Section 5.1 WP257

Please confirm and explain how your BCR for Processors allow for informing other parts of the Group, the concerned Supervisory Authorities via the competent SA under Article 64 (i.e. the BCR Lead) and data controllers of any changes to the BCR for Processors and/or the list of BCR members (summary):

Please confirm that you have put in place a system to record any changes to your BCR for Processors.

Please confirm that where a change affects the processing conditions, data controllers are informed in a timely fashion that data controllers have the possibility to object to the changes or terminate the contract before the modification is made

9. DATA PROTECTION SAFEGUARDS[21]

Please, specify with reference to your BCR for Processors how and where the following issues are addressed with supporting documentation where appropriate:

- Transparency, fairness and lawfulness (e.g., general duty to help and assist the controller)

- Purpose limitation (e.g., duty to process personal data only on behalf of data controllers and in compliance with their instructions and to return the data to the data controller at the end of the contract)

- Data quality (e.g., general duty to help and assist the controller)

- Security

- Data subjects' rights (e.g., general duty to help and assist the controller)

- Subprocessing within the Group

- Restrictions on onward transfers to external subprocessors

- Other (e.g. protection of children, etc.)

[21] See Section 6 of WP257

10. ACCOUNTABILITY AND OTHER TOOLS[22]
-Please confirm and specify how BCR members will make available to the controller all information necessary to demonstrate compliance with their obligations as provided by Article 28-3-h (including through audits, and information of the controller if an instruction infringes the GDPR or other Union or Member State data protection provisions) -Please confirm that the BCR members will maintain a record of all categories of processing activities carried out on behalf of each controller as provided by Article 30-2 GDPR -Please specify how BCR members will assist the controller in implementing appropriate technical and organisational measures to comply with data protection principles and facilitate compliance with requirements set out by BCRs in practice (e.g. data protection by design, data protection by default) Please provide supporting documents where appropriate with respect to the information requested above

[22] See Section 6.1.2 WP257

ANNEX 1:
COPY OF THE FORMAL BINDING CORPORATE RULES FOR PROCESSORS

Please attach a copy of your BCR for Processors. Note that this does not include any ancillary documentation that you would like to submit (e.g. specific privacy policies and rules).

ARTICLE 29 DATA PROTECTION WORKING PARTY

WORKING PARTY 29 POSITION PAPER on the derogations from the obligation to maintain records of processing activities pursuant to Article 30(5) GDPR

The Working Party 29 has examined the obligation, under Article 30 of the GDPR, for controllers and processors to maintain a record of processing activities. This paper sets out the WP29's position on the derogation from this obligation.

Recital 13 of the GDPR says:

'To take account of the specific situation of micro, small and medium-sized enterprises, this Regulation includes a derogation for organisations with fewer than 250 employees with regard to record-keeping'.

Article 30(5) gives effect to Recital 13. It says that the obligation to keep a record of processing activities does not apply *'to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.'*

Some clarifications on the interpretation of this provision appear necessary, as shown by the high number of requests coming from companies and received in the last few months by national Supervisory Authorities.

The derogation provided by Article 30(5) is not absolute. There are three types of processing to which it does not apply. These are:

- Processing that is likely to result in a risk to the rights and freedoms of data subjects.
- Processing that is not occasional.
- Processing that includes special categories of data or personal data relating to criminal convictions and offences.

The WP29 underlines that the wording of Article 30(5) is clear in providing that the three types of processing to which the derogation does not apply are alternative ("or") and the occurrence of any one of them alone triggers the obligation to maintain the record of processing activities.

Therefore, although endowed with less than 250 employees, data controllers or processors who find themselves in the position of either carrying out processing likely to result in a risk (not just a high risk) to the rights of the data subjects, or processing personal data on a non-occasional basis, or processing special categories of data under Article 9(1) or data relating to criminal convictions under Article 10 are obliged to maintain the record of processing activities.

However, such organisations need only maintain records of processing activities for the types of processing mentioned by Article 30(5).

For example, a small organisation is likely to regularly process data regarding its employees. As a result, such processing cannot be considered "occasional" and must therefore be included in the record of processing activities.[1] Other processing activities which are in fact "occasional", however, do not need to be included in the record of processing activities, provided they are unlikely to result in a risk to the right and freedoms of data subjects and do not involve special categories of data or personal data relating to criminal convictions and offences.

The WP29 highlights that the record of processing activities is a very useful means to support an analysis of the implications of any processing whether existing or planned. The record facilitates the factual assessment of the risk of the processing activities performed by a controller or processor on individuals' rights, and the identification and implementation of appropriate security measures to safeguard personal data – both key components of the principle of accountability contained in the GDPR.

For many micro, small and medium-sized organisations, maintaining a record of processing activities is unlikely to constitute a particularly heavy burden. However, the WP29 recognises that Article 30 represents a new administrative requirement for controllers and processors, and therefore encourages national Supervisory Authorities to support SMEs by providing tools to facilitate the set up and management of records of processing activities. For example, a Supervisory Authority might make available on its website a simplified model that can be used by SMEs to keep records of processing activities not covered by the derogation in Article 30(5).

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate C (Fundamental Rights and Union Citizenship) of the European Commission, Directorate General Justice, B-1049 Brussels, Belgium, Office No MO-59 02/013.

Website: http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358&tpa_id=6936

[1] The WP29 considers that a processing activity can only be considered as "occasional" if it is not carried out regularly, and occurs outside the regular course of business or activity of the controller or processor. See WP29 Guidelines on Article 49 of Regulation 2016/679 (WP262).

ARTICLE 29 DATA PROTECTION WORKING PARTY

17/EN
WP263 rev.01

Working Document Setting Forth a Co-Operation Procedure for the approval of "Binding Corporate Rules" for controllers and processors under the GDPR

Adopted on 11 April 2018

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.
The secretariat is provided by Directorate C (Fundamental Rights and Union Citizenship) of the European Commission, Directorate General Justice, B-1049 Brussels, Belgium, Office No MO-59 02/013.
Website: http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358&tpa_id=6936

ARTICLE 29 DATA PROTECTION WORKING PARTY

Introduction

The procedure for approving binding corporate rules (BCRs) for controllers and processors is laid out by provisions contained in Articles 47.1, 63, 64 and (only if necessary) 65 of the Regulation (EU) 2016/679 (GDPR).

As a result, binding corporate rules are to be approved by the competent supervisory authority[1] in the relevant jurisdiction in accordance with the consistency mechanism set out in Article 63, under which the European Data Protection Board (EDPB) will issue a non-binding opinion on the draft decision submitted by the competent Supervisory Authority (Article 64 GDPR).

As the group applying for approval of its BCRs may have entities in more than one Member State, this procedure may involve a number of concerned Supervisory Authorities (SAs)[2], e.g. in those countries from where the transfers are to take place. However, the GDPR does not lay down specific rules for the cooperation phase which should take place among the concerned SAs in advance of referral to the EDPB. It also does not set out specific rules for identifying the competent SA – which will act as Lead Authority for the BCRs ('BCR Lead')[3]. The role of such BCR Lead includes acting as a single point of contact with the applicant organization or group during the approval process and managing the application procedure in its cooperation phase.

The aim of this document is to update the WP 107 and identify smooth and effective cooperation procedures in line with the GDPR whilst taking full advantage of the previous fruitful experience of the Data Protection Authorities in dealing with the approval of BCRs.

This document will be reviewed and if necessary updated, based on the practical experience gained through the application of the GDPR.

[1] Article 57.1.s GDPR states that "without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory […] approve binding corporate rules pursuant to Article 47" and Article 58.3.j GDPR according to which each supervisory authority shall have the "authorisation and advisory powers […] to approve binding corporate rules pursuant to Article 47".

[2] Pursuant to Article 4(22) (a) and (b), a 'supervisory authority concerned' means a supervisory authority which is concerned by the processing of personal data because the controller or processor is established on the territory of the Member State of that supervisory authority or because "data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing". As for the BCRs approval procedure, the concerned SAs are the SAs in the countries from where the transfers are to take place as specified by the applicants or, in case of BCR-P, all SAs (since a processor established in a Member State may provide services to controllers in several – potentially all – Member States).

[3] The "BCR Lead" is generally distinct from the "OSS Lead" considering that BCR transfers will not as a rule meet the definition/criteria of a cross-border processing operation. However, there could be cases in which the same SA could be the BCR Lead and the OSS Lead. This might e.g. be the case if a transfer performed by one establishment substantially affects data subjects in more than one MS (i.e. if personal data are first sent from member states A, B and C to the controller's establishment in member state A, and subsequently transferred by this establishment in A to a third country or, in case of BCR-P, where the processor carries out the same transfers for all their clients in the different member states). In any case, the BCR approval procedure would be the specific one settled by Article 64 GDPR.

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.
The secretariat is provided by Directorate C (Fundamental Rights and Union Citizenship) of the European Commission, Directorate General Justice, B-1049 Brussels, Belgium, Office No MO-59 02/013.
Website: http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358&tpa_id=6936

1. Identification of the BCR Lead Supervisory Authority

1.1 A group of undertakings, or group of enterprises engaged in a joint economic activity ('Group'), interested in submitting draft binding corporate rules (BCRs) for the approval of the competent Authority according to Articles 47, 63 and 64 GDPR should propose a SA as the BCR Lead. The decision as to which SA should act as BCR Lead is based upon the criteria contained in this document (see next paragraph). It is for the organisation to justify the reasons why a given SA should be considered as the BCR Lead.

1.2 An applicant Group should justify the proposal of the BCR Lead on the basis of relevant criteria such as:

a. the location(s) of the Group's European headquarters;

b. the location of the company within the Group with delegated data protection responsibilities[4];

c. the location of the company which is best placed (in terms of management function, administrative burden, etc.) to deal with the application and to enforce the binding corporate rules in the Group;

d. the place where most decisions in terms of the purposes and the means of the processing (i.e. transfer) are taken; and

e. the member state within the EU from which most or all transfers outside the EEA will take place.

1.3 Particular attention will be given to factor described under 1.2 (a) above.

1.4 These are not formal criteria. The SA to which the application is sent (as prospective BCR Lead SA) will exercise its discretion in deciding whether it is in fact the most appropriate lead SA and, in any event, the SAs among themselves may decide to allocate the application to a SA other than the one to which the Group applied (see next paragraph), in particular if it would be possible and worth for speeding up the procedure (e.g. taking into account the workload of the originally requested SA).

[4] According to Article 47.2.f GDPR, there should always be an EU based member of the group established on the territory of a Member State accepting liability for any breaches of the binding corporate rules by any member concerned not established in the Union. If the headquarters of the group were somewhere else, the headquarters should delegate these responsibilities to a member based in the EU.

ARTICLE 29 DATA PROTECTION WORKING PARTY

1.5 The applicant should also provide the proposed BCR Lead (the entry point) with all appropriate information (both on paper and electronically to facilitate further distribution) which justifies its proposal, *inter alia*, the nature and general structure of the processing activities in the EU with particular attention to the place/s where decisions are made, the location and nature of affiliates in the EU, the number of employees or persons concerned, the means and purposes of the processing, the places from where the transfers to third countries do take place and the third countries to which those data are transferred.

2. **Cooperation procedure for the approval of BCRs**

2.1 The proposed BCR Lead will forward the information received as to why that SA has been selected by the company to be the lead authority for the BCRs to all SAs concerned[5] with an indication of whether or not it agrees to be the BCR Lead. If the entry point agrees to be the lead authority, the other concerned SAs will be asked, under Article 57.1.g GDPR, to raise any objections within two weeks (period extendable to two additional weeks if requested by any SA concerned). Silence is deemed as consent. In the event that the entry point is of the view that it should not act as the BCR Lead, it should explain the reasons for its decision as well as its recommendations (if any) as to which other SA would be the appropriate lead authority. The SAs concerned will endeavor to reach a decision within one month from the date that the papers were first circulated.

2.2 Once a decision on the BCR Lead has been made, the latter will start the discussions with the applicant and review the draft BCR documents. In order to foster a more consistent approach, it will send, under Article 57.1.g GDPR, a first revised draft of the BCRs and the related documents to one or two SAs (depending on the number of Member States from whose territories the transfers will take place)[6] which will act as co-reviewers and will help the BCR Lead in the assessment. In case there is no response from a SA acting as co-reviewer within one month from the date the draft and the related documents were sent to it (deadline extendable under justified circumstances), that SA will be deemed to have agreed with them. There may need to be several different drafts or exchanges between the applicant and the relevant SAs before a satisfactory draft is produced.

2.3 The result of these discussions should be a "consolidated draft" sent by the applicant to the BCR Lead which will circulate it among all concerned SAs[7] under Article 57.1.g GDPR for comments. According to this procedure, the period for comments on the consolidated draft will not exceed one month. A concerned SA which has not presented a

[5] See above footnote n. 2.
[6] As a rule, the BCR Lead will consult 2 co-reviewers whenever 14 Member States or more are concerned by transfers. Under this threshold it is possible to have one or two co-reviewers depending on the specific case and the availability of SAs.
[7] See above footnote n. 2.

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.
The secretariat is provided by Directorate C (Fundamental Rights and Union Citizenship) of the European Commission, Directorate General Justice, B-1049 Brussels, Belgium, Office No MO-59 02/013.
Website: http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358&tpa_id=6936

reasoned objection within this period shall be deemed to be in agreement with the consolidated draft.

2.4 The BCR Lead will send any further comments on the "consolidated draft" to the applicant and may resume discussions, if necessary. If the lead authority is of the view that the applicant is in a position to address satisfactorily all comments received, it will invite the applicant to send a "final draft" to it.

2.5 Pursuant to Article 64.1 and 64.4 GDPR, the BCR Lead will submit the draft decision to the EDPB on the 'final draft' of the BCRs along with all relevant information, documentation and the views of the concerned SAs. The EDPB will adopt an opinion on the matter in accordance with Article 64.3 GDPR and its Rules of Procedure.

2.6 Where the opinion handed down by the EDPB under Article 64.3 endorses the draft decision on the draft BCRs in the form submitted, the BCR Lead will adopt its decision approving the draft BCRs.

2.7 Where the opinion handed down by the EDPB according to Article 64.3 requires any amendment to the draft BCRs, the BCR Lead will communicate to the Chair of the Board within the two-week period set out in Article 64.7 whether it intends to maintain its draft decision (i.e. not to follow the opinion of the EDPB) or whether it intends to amend it in accordance with the EDPB opinion[8]. In the first case, pursuant to Article 64.8 GDPR, Article 65.1 GDPR shall apply[9]. If the BCR Lead communicates to the Chair of the Board that it intends to amend its draft decision in accordance with the EDPB opinion, the BCR Lead will contact the applicant immediately in order to request the amendments to the draft BCRs to be made in accordance with the EDPB opinion so that the draft BCRs can be finalized. When the draft BCRs have been finalized in accordance with the EDPB opinion, the BCR Lead will amend its initial draft decision accordingly, notify the EDPB pursuant Article 64.7 of its amended decision and approve the BCR.

2.8 Once the BCR Lead approves the BCRs, it will inform and send a copy of them to all the concerned SAs. In accordance with Article 46.2.b GDPR, the approved 'binding corporate rules' will provide for the appropriate safeguards referred to in paragraph 46.1 without requiring any specific authorisation from the other concerned supervisory authorities.

2.9 Translations: as a general rule and without prejudice to other translations where necessary or

[8] According to Article 64.5, the Chair of the Board will, without undue delay, inform by electronic means the members of the Board and the Commission of this information.

[9] In particular, in accordance with Article 65.1.c., "in order to ensure the correct and consistent application of this Regulation in individual cases, the Board shall adopt a binding decision in the following cases: [...] (c) where a competent supervisory authority [...] does not follow the opinion of the Board issued under Article 64. In that case, any supervisory authority concerned or the Commission may communicate the matter to the Board".

required by law, all documents including the consolidated draft of the BCRs should be provided by the applicant in the language of the BCR Lead and also in English when possible in accordance with national law. The final draft and the approved BCRs must be translated by the applicant into the languages of those SAs concerned[10].

2.10 Once the BCRs have been approved, the BCR Lead, according to WP 256 and 257, points 5.1, will inform the concerned SAs of any updates to the BCRs or to the list of BCR members as provided by the applicant. In case the group extended the scope of the BCRs to an additional EU member state (because of the establishment of a new BCR member in this EU member state), the SA of this member state will then be deemed to be a new concerned SA as for point 2.8.

[10] See also on this WP 256 and 257, Sections 1.7 according to which "The BCRs must contain the right for every data subject to have an easy access to them".

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.
The secretariat is provided by Directorate C (Fundamental Rights and Union Citizenship) of the European Commission, Directorate General Justice, B-1049 Brussels, Belgium, Office No MO-59 02/013.
Website: http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358&tpa_id=6936

GRUPA ROBOCZA ART. 29

18/PL
WP 256 rev.01

Dokument roboczy ustanawiający tabelę zawierającą elementy i zasady, które mają zostać uwzględnione w wiążących regułach korporacyjnych

Przyjęty dnia 28 listopada 2017 r.
Ostatnio zmieniony i przyjęty w dniu 6 lutego 2018 r.

Grupa Robocza została powołana na mocy art. 29 dyrektywy 95/46/WE. Jest ona niezależnym europejskim organem doradczym w zakresie ochrony danych i prywatności. Zadania Grupy zostały określone w przepisach art. 30 dyrektywy 95/46/WE i art. 15 dyrektywy 2002/58/WE.

Obsługę sekretariatu zapewnia Dyrekcja C (Prawa Podstawowe i Obywatelstwo Unii Europejskiej) Dyrekcji Generalnej ds. Sprawiedliwości, B-1049 Bruksela, Belgia, biuro nr MO-59 02/013.

Strona internetowa: http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358&tpa_id=6936

WPROWADZENIE

Aby ułatwić korzystanie z wiążących reguł korporacyjnych dla administratorów przez grupy przedsiębiorstw lub grupy przedsiębiorców prowadzących wspólną działalność gospodarczą do celów międzynarodowego przekazywania danych z organizacji posiadających jednostkę organizacyjną w UE do organizacji należących do tej samej grupy i posiadających jednostkę organizacyjną poza UE, Grupa Robocza Art. 29 (GR29) zmieniła dokument roboczy WP 153 (przyjęty w 2008 r.) ustanawiający tabelę zawierającą elementy i zasady, które mają być uwzględnione w wiążących regułach korporacyjnych, aby odzwierciedlić wymogi odnoszące się do wiążących reguł korporacyjnych, obecnie wyraźnie określonych w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE („ogólne rozporządzenie o ochronie danych" / „RODO")[1].

Należy przypomnieć, że wiążące reguły korporacyjne dla administratorów są odpowiednie do regulowania przekazywania danych osobowych przez administratorów posiadających jednostkę organizacyjną w UE innym administratorom lub podmiotom przetwarzającym (posiadającym jednostkę organizacyjną poza UE) należącym do tej samej grupy, podczas gdy wiążące reguły korporacyjne dla podmiotów przetwarzających mają zastosowanie do danych otrzymanych od administratora (posiadającego jednostkę organizacyjną w UE), który nie jest członkiem tej grupy, a następnie przetworzonych przez członków przedmiotowej grupy działających w charakterze podmiotów przetwarzających lub podprzetwarzających. A zatem obowiązki określone w wiążących regułach korporacyjnych dla administratorów mają zastosowanie w odniesieniu do podmiotów należących do tej samej grupy działających w charakterze administratorów oraz do podmiotów działających w charakterze „wewnętrznych" podmiotów przetwarzających. Jeżeli chodzi o podmioty działające w charakterze „wewnętrznych" podmiotów przetwarzających, warto przypomnieć, że umowy lub inne instrumenty prawne przyjęte na podstawie prawa unijnego lub prawa państwa członkowskiego mające charakter wiążący dla podmiotu przetwarzającego w odniesieniu do administratora oraz zawierające wszystkie wymogi określone w art. 28 ust. 3 RODO powinny zostać podpisane ze wszystkimi wewnętrznymi i zewnętrznymi podwykonawcami / podmiotami przetwarzającymi (np. umowa o świadczenie usług lub inne instrumenty spełniające te same wymagania)[2]. Obowiązki określone w wiążących regułach korporacyjnych dla administratorów mają zastosowanie do podmiotów należących do grupy otrzymujących dane osobowe, które działają w charakterze („wewnętrznych") podmiotów przetwarzających, w takim zakresie, w jakim nie prowadzi to do wystąpienia sprzeczności z umową o świadczenie usług (tzn. umowy tej przestrzegają przede wszystkim członkowie grupy pełniący funkcję podmiotów przetwarzających, którzy przetwarzają dane w imieniu członków grupy pełniących funkcje administratorów).

[1] Tekst mający znaczenie dla EOG.
[2] W art. 28 ust. 3 nałożono między innymi wymóg określenia – w odniesieniu do każdej relacji administrator-podmiot przetwarzający – za pomocą umowy lub innego instrumentu prawnego: przedmiotu, czasu trwania, charakteru i celów przetwarzania danych, rodzaju danych osobowych oraz kategorii osób, których dane dotyczą, a także obowiązków i praw administratora. Zawarcie w wiążących regułach korporacyjnych ogólnego opisu w odniesieniu do kategorii danych, osób, których dane dotyczą, itd. nie byłoby pod tym względem wystarczające.

Biorąc pod uwagę, że w art. 47 ust. 2 RODO określono minimalny zestaw elementów, które należy zawrzeć w wiążących regułach korporacyjnych, niniejsza zmieniona tabela ma służyć:

- dostosowaniu brzmienia poprzedniej listy referencyjnej, aby zapewnić jej zgodność z art. 47 RODO;
- wyjaśnieniu niezbędnej treści wiążących reguł korporacyjnych, jak określono w art. 47 RODO (z uwzględnieniem dokumentów WP 74[3] i WP 108[4] przyjętych przez GR29 w ramach dyrektywy 95/46/WE);
- rozróżnieniu elementów, które należy zawrzeć w wiążących regułach korporacyjnych, od elementów, które należy przedstawić właściwemu organowi nadzorczemu we wniosku w sprawie wiążących reguł korporacyjnych (dokument roboczy WP 133[5]);
- opatrzeniu zasad odpowiadającymi im odniesieniami do treści art. 47 RODO; oraz
- przedstawieniu wyjaśnień/uwag dotyczących każdej z zasad.

Art. 47 RODO został wyraźnie opracowany w oparciu o dokumenty robocze dotyczące wiążących reguł korporacyjnych przyjęte przez GR29. W RODO określono jednak pewne nowe elementy, które należy wziąć pod uwagę przy aktualizowaniu już istniejących wiążących reguł korporacyjnych lub przy przyjmowaniu nowych zestawów wiążących reguł korporacyjnych, aby zapewnić ich zgodność z nowymi ramami określonymi przez RODO.

1.1 Nowe elementy

W związku z tym GR29 chciałaby zwrócić uwagę w szczególności na następujące elementy:

- ***prawo do wniesienia skargi:*** osoby, których dane dotyczą, powinny mieć prawo wnieść skargę – według własnego uznania – albo do organu nadzorczego w państwie członkowskim swojego zwykłego pobytu, swojego miejsca pracy lub miejsca popełnienia domniemanego naruszenia (zgodnie z art. 77 RODO), albo do właściwego sądu z danego państwa członkowskiego UE (osoba, której dane dotyczą, może wybrać postępowanie przed sądami znajdującymi się w miejscu, w którym podmiot przekazujący dane ma jednostkę organizacyjną lub które jest miejscem zwykłego pobytu osoby, której dane dotyczą) (art. 79 RODO);
- ***przejrzystość:*** wszystkim osobom, których dane dotyczą i które korzystają z praw beneficjenta będącego osobą trzecią, należy przekazać w szczególności informacje określone w art. 13 i 14 RODO oraz informacje o prawach tych osób w zakresie przetwarzania danych i środkach egzekwowania tych praw, informacje na temat klauzuli dotyczącej odpowiedzialności prawnej i klauzul dotyczących zasad ochrony danych;

[3] Dokument roboczy WP 74: „Przekazywanie danych osobowych do państw trzecich: stosowanie art. 26 ust. 2 dyrektywy UE o ochronie danych do wiążących reguł korporacyjnych w odniesieniu do międzynarodowego przekazywania danych", przyjęty w dniu 3 czerwca 2003 r.: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp74_en.pdf

[4] Dokument roboczy WP 108 ustanawiający wzór wniosku o zatwierdzenie wiążących reguł korporacyjnych mającego formę listy kontrolnej, przyjęty w dniu 14 kwietnia 2005 r.: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp108_en.pdf

[5] Dokument roboczy WP 133: Zalecenie nr 1/2007 w sprawie standardowego wniosku o zatwierdzenie wiążących reguł korporacyjnych w odniesieniu do przekazywania danych osobowych, przyjęte w dniu 10 stycznia 2007 r.: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp133_en.doc

- ***zakres stosowania:*** w wiążących regułach korporacyjnych określa się strukturę i dane kontaktowe odnośnej grupy przedsiębiorstw lub grupy przedsiębiorców prowadzących wspólną działalność gospodarczą i każdego z jej członków (art. 47 ust. 2 lit. a) RODO). W wiążących regułach korporacyjnych należy również określić materialny zakres stosowania, którym jest przykładowo jednorazowe lub wielokrotne przekazanie danych, w tym kategorie danych osobowych, rodzaj przetwarzania i jego cele, rodzaje osób, których dane dotyczą, oraz nazwa danego państwa trzeciego lub danych państw trzecich (art. 47 ust. 2 lit. b) RODO);
- ***zasady ochrony danych:*** w wiążących regułach korporacyjnych oprócz zasad przejrzystości, rzetelności, ograniczenia celu, jakości danych i bezpieczeństwa należy również wyjaśnić pozostałe zasady, o których mowa w art. 47 ust. 2 lit. d), takie jak w szczególności zasady zgodności z prawem, minimalizacji danych, ograniczonych okresów przechowywania, gwarancji w przypadku przetwarzania szczególnych kategorii danych osobowych, wymogi w zakresie dalszego przekazywania danych podmiotom niezwiązanym wiążącymi regułami korporacyjnymi;
- ***rozliczalność:*** każdy podmiot działający w charakterze administratora danych jest odpowiedzialny za przestrzeganie wiążących reguł korporacyjnych i musi być w stanie wykazać ich przestrzeganie (art. 5 ust. 2 RODO);
- ***prawodawstwo państw trzecich:*** wiążące reguły korporacyjne powinny zawierać zobowiązanie do tego, aby – w przypadku gdy jakikolwiek wymóg prawny, któremu podlega w państwie trzecim członek grupy przedsiębiorstw lub grupy przedsiębiorców prowadzących wspólną działalność gospodarczą i który może mieć istotny niekorzystny wpływ na gwarancje przewidziane w wiążących regułach korporacyjnych – problem ten zgłaszać właściwemu organowi nadzorczemu (chyba że jest to zakazane na mocy innego przepisu, na przykład na mocy prawa karnego w celu zachowania poufności postępowania prowadzonego przez organy ścigania). Obejmuje to wszelkie prawnie wiążące wnioski o ujawnienie danych osobowych wystosowane przez organ ścigania lub organ ds. bezpieczeństwa państwa.

1.2 Zmiany przyjętych wcześniej wiążących reguł korporacyjnych

Chociaż zgodnie z art. 46 ust. 5 RODO zezwolenia wydane przez państwo członkowskie lub organ nadzorczy na podstawie art. 26 ust. 2 dyrektywy 95/46/WE zachowują ważność do czasu ich zmiany – w razie potrzeby – przez ten organ, bądź też ich zastąpienia lub uchylenia, grupy, których wiążące reguły korporacyjne zostały zatwierdzone, przygotowując się do zastosowania RODO, powinny dostosować te reguły do wymogów RODO.

Niniejszy dokument ma także pomóc tym grupom, których wiążące reguły korporacyjne zostały zatwierdzone, we wdrożeniu istotnych zmian, aby dostosować je do RODO. Dlatego też grupy te zachęca się do tego, by w ramach spoczywającego na nich (na podstawie pkt 5. 1 dokumentu roboczego WP 153) obowiązku powiadamiały wszystkich członków grupy i organy ochrony danych poprzez wiodący organ ochrony danych o istotnych zmianach poczynionych w swoich wiążących regułach korporacyjnych w ramach corocznej aktualizacji, począwszy od dnia 25 maja 2018 r. Stosowanie takich zaktualizowanych wiążących reguł korporacyjnych nie wiąże się z obowiązkiem złożenia wniosku o dokonanie nowej autoryzacji lub zatwierdzenia.

Biorąc pod uwagę powyższe informacje, organy ochrony danych zastrzegają sobie prawo do korzystania ze swoich uprawnień na podstawie art. 46 ust. 5 RODO.

GRUPA ROBOCZA ART. 29

Kryteria zatwierdzenia wiążących regul korporacyjnych	W wiążących regułach korporacyjnych	W formularzu wniosku	Teksty odniesienia	Uwagi	Odniesienia do wniosku / wiążących regul korporacyjnych[6]
1 – CHARAKTER WIĄŻĄCY					
WEWNĘTRZNY					
1.1 Obowiązek przestrzegania wiążących regul korporacyjnych	TAK	TAK	Art. 47 ust. 1 lit. a) oraz art. 47 ust. 2 lit. c) RODO	Wiążące reguły korporacyjne muszą być prawnie wiążące; reguły te powinny także zawierać wyraźny obowiązek ich przestrzegania przez każdego członka grupy przedsiębiorstw lub grupy przedsiębiorców prowadzących wspólną działalność gospodarczą („członek, którego dotyczą wiążące reguły korporacyjne"), w tym ich pracowników.	
1.2 Wyjaśnienie sposobu nadawania regułom wiążącego charakteru w odniesieniu do członków grupy, których dotyczą te reguły, a także pracowników	NIE	TAK	Art. 47 ust. 1 lit. a) oraz art. 47 ust. 2 lit. c) RODO	W formularzu wniosku grupa będzie musiała wyjaśnić, w jaki sposób nadaje regułom charakter wiążący: (i) w przypadku każdego uczestniczącego przedsiębiorstwa/podmiotu z grupy – za pomocą co najmniej jednego/jednej: - umowy wewnątrzgrupowej; - jednostronnego zobowiązania (jest to możliwe wyłącznie wtedy, gdy członek, którego dotyczą wiążące reguły korporacyjne, przyjmujący na siebie zobowiązania i odpowiedzialność prawną znajduje się w państwie członkowskim, które uznaje jednostronne zobowiązania za wiążące, i gdy członek ten posiada zdolność prawną do podejmowania zobowiązań za pozostałych członków, których dotyczą wiążące reguły korporacyjne); - innego środka (wyłącznie jeżeli grupa wykaże, w jaki sposób wiążące reguły korporacyjne nabywają charakter wiążący); (ii) w przypadku pracowników – za pomocą co najmniej jednego/jednej: - indywidualnej i odrębnej umowy przewidującej sankcje / indywidualnego i odrębnego zobowiązania przewidującego sankcje; - klauzuli w umowie o pracę zawierającej opis mających zastosowanie sankcji; - wewnętrznej polityki przewidującej sankcje; lub - układu zbiorowego przewidującego sankcje; - innego środka (jednak grupa musi odpowiednio wyjaśnić, w jaki sposób nadaje się wiążący charakter wiążącym regułom korporacyjnym w odniesieniu do	

[6] Wypełnia wnioskodawca.

Grupa Robocza została powołana na mocy art. 29 dyrektywy 95/46/WE. Jest ona niezależnym europejskim organem doradczym w zakresie ochrony danych i prywatności. Zadania Grupy zostały określone w przepisach art. 30 dyrektywy 95/46/WE i art. 15 dyrektywy 2002/58/WE.

Obsługę sekretariatu zapewnia Dyrekcja C (Prawa Podstawowe i Obywatelstwo Unii Europejskiej) Dyrekcji Generalnej ds. Sprawiedliwości, B-1049 Bruksela, Belgia, biuro nr MO-59 02/013.

Strona internetowa: http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358&tpa_id=6936

Kryteria zatwierdzenia wiążących regul korporacyjnych	W wiążących regułach korporacyjnych	W formularzu wniosku	Teksty odniesienia	Uwagi	Odniesienia do wniosku / wiążących regul korporacyjnych[6]

Kryteria zatwierdzenia wiążących regul korporacyjnych	W wiążących regułach korporacyjnych	W formularzu wniosku	Teksty odniesienia	Uwagi	Odniesienia do wniosku / wiążących regul korporacyjnych[6]
				pracowników).	
ZEWNĘTRZNY					
1.3 Ustanowienie praw beneficjenta będącego osobą trzecią w odniesieniu do osób, których dane dotyczą, w tym możliwości wniesienia skargi do właściwego organu nadzorczego i sądu	TAK	TAK	Art. 47 ust. 1 lit. b), art. 47 ust. 2 lit. c) i e) RODO	W wiążących regułach korporacyjnych należy wyraźnie określić prawa osób, których dane dotyczą, do egzekwowania - jako beneficjenci będący osobami trzecimi – tych reguł. Osoby, których dane dotyczą, muszą być w stanie wyegzekwować co najmniej następujące elementy wiążących reguł korporacyjnych: - zasady ochrony danych (art. 47 ust. 2 lit. d) RODO oraz sekcja 6.1 niniejszego dokumentu); - przejrzystość i łatwy dostęp do wiążących reguł korporacyjnych (art. 47 ust. 2 lit. g) RODO oraz sekcje 6.1 i 1.7 niniejszego dokumentu); - prawo dostępu, sprostowania i usunięcia danych, ograniczenia przetwarzania, prawo do sprzeciwu wobec przetwarzania, prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym na profilowaniu (art. 47 ust. 2 lit. e) i art. 15, 16, 17, 18, 21, 22 RODO); - prawodawstwo krajowe uniemożliwiające przestrzeganie wiążących regul korporacyjnych (art. 47 ust. 2 lit. m) RODO oraz sekcja 6.3 niniejszego dokumentu); - prawo do złożenia skargi za pośrednictwem	

7

Kryteria zatwierdzenia wiążących regul korporacyjnych	W wiążących regułach korporacyjnych	W formularzu wniosku	Teksty odniesienia	Uwagi	Odniesienia do wniosku / wiążących regul korporacyjnych[6]
				wewnętrznego mechanizmu wnoszenia skarg stosowanego przez przedsiębiorstwa (art. 47 ust. 2 lit. i) RODO oraz sekcja 2.2 niniejszego dokumentu); - obowiązki związane ze współpracą z organami nadzorczymi (art. 47 ust. 2 lit. k) oraz l) RODO, a także sekcja 3.1 niniejszego dokumentu); - przepisy dotyczące odpowiedzialności prawnej i jurysdykcji (art. 47 ust. 2 lit. e) i f) RODO oraz sekcje 1.3 i 1.4 niniejszego dokumentu). W wiążących regułach korporacyjnych musi zostać w szczególności przyznane prawo do wniesienia skargi do właściwego organu nadzorczego (zgodnie z art. 77 RODO można wybrać organ nadzorczy w państwie członkowskim swojego zwykłego pobytu, miejsca pracy lub miejsca popełnienia domniemanego naruszenia) i do właściwego sądu z danego państwa członkowskiego UE (zgodnie z art. 79 RODO osoba, której dane dotyczą, może zdecydować się wszcząć postępowanie przed sądem państwa członkowskiego, w którym administrator lub podmiot przetwarzający posiadają jednostkę organizacyjną, lub przed sądem państwa członkowskiego, w którym osoba, której dane dotyczą, ma miejsce zwykłego pobytu). W wiążących regułach korporacyjnych należy wyraźnie przyznać osobom, których dane dotyczą, prawo do środków zaskarżenia i prawo do otrzymania zadośćuczynienia oraz – w stosownych przypadkach – odszkodowania	

8

Kryteria zatwierdzenia wiążących reguł korporacyjnych	W wiążących regułach korporacyjnych	W formularzu wniosku	Teksty odniesienia	Uwagi	Odniesienia do wniosku / wiążących reguł korporacyjnych[6]
				w przypadku naruszenia jednego z możliwych do wyegzekwowania na drodze prawnej wymienionych powyżej elementów wiążących reguł korporacyjnych (zob. art. 77–82 RODO). Przedsiębiorstwa powinny zapewnić, aby wszystkie prawa zostały objęte klauzulą dotyczącą beneficjenta będącego osobą trzecią zawartą w wiążących regułach korporacyjnych tych przedsiębiorstw, przykładowo odnosząc się do klauzul/sekcji/części tych reguł, w których uregulowano te prawa, lub wymieniając je wszystkie w przedmiotowej klauzuli dotyczącej beneficjenta będącego osobą trzecią. Prawa te nie obejmują tych elementów wiążących reguł korporacyjnych, które dotyczą wewnętrznych mechanizmów wdrożonych przez podmioty, takich jak dane szczegółowe szkoleń, programów audytu, sieci zgodności i mechanizmu aktualizowania tych reguł.	
1.4 Siedziba główna w UE, członkowie z UE, którym przekazano obowiązki ochrony danych, lub podmiot przekazujący dane przyjmują odpowiedzialność prawną za wypłatę odszkodowania oraz usunięcie naruszeń wiążących reguł korporacyjnych	TAK	TAK	Art. 47 ust. 2 lit. f) RODO	Wiążące reguły korporacyjne muszą zawierać obowiązek nałożony na siedzibę główną w UE lub na członka z UE, którego te reguły dotyczą i któremu przekazano obowiązki, do przyjęcia odpowiedzialności za działania innych członków spoza UE związanych wiążącymi regułami korporacyjnym oraz za podjęcie niezbędnych kroków w celu ich naprawienia, jak również do przyjęcia odpowiedzialności za wypłatę odszkodowania za wszelkie szkody materialne lub niematerialne wynikające z naruszenia wiążących reguł korporacyjnych przez członków, których te reguły dotyczą. W wiążących regułach korporacyjnych należy również stwierdzić, że w przypadku gdy członek	

Kryteria zatwierdzenia wiążących reguł korporacyjnych	W wiążących regułach korporacyjnych	W formularzu wniosku	Teksty odniesienia	Uwagi	Odniesienia do wniosku / wiążących reguł korporacyjnych[6]
				spoza UE, którego dotyczą te reguły, naruszy wiążące reguły korporacyjne, jurysdykcję będą sprawowały sądy lub inne właściwe organy w UE, a osobie, której dane dotyczą, będą przysługiwać takie prawa i środki ochrony prawnej wobec członka, którego dotyczą te reguły i który przyjął na siebie zobowiązania i odpowiedzialność prawną, jak gdyby naruszenie to popełnił członek w państwie członkowskim, w którym jest zlokalizowany, a nie członek spoza UE, którego dotyczą te reguły. Inna możliwość – szczególnie w przypadku, gdy dana grupa o szczególnych strukturach korporacyjnych nie może całkowicie obciążyć konkretnego podmiotu odpowiedzialnością za jakiekolwiek naruszenie wiążących reguł korporacyjnych poza UE – może polegać na tym, że każdy członek, którego te reguły dotyczą i który na ich podstawie eksportuje dane poza UE, będzie odpowiedzialny prawnie za wszelkie naruszenia tych reguł przez członka, którego te reguły dotyczą, który jest zlokalizowany poza UE oraz który otrzymał dane od tego członka z UE, którego dotyczą wiążące reguły korporacyjne.	
1.5 Przedsiębiorstwo posiada wystarczające aktywa	NIE	TAK	[WP 74 pkt 5.5.2 akapit drugi (s. 18) + WP 108 pkt 5.17 (s. 6)]	Formularz wniosku musi zawierać potwierdzenie faktu, że każdy członek, którego dotyczą wiążące reguły korporacyjne i który przyjął na siebie odpowiedzialność prawną za działania innych członków spoza UE, których dotyczą wiążące reguły korporacyjne, posiada wystarczające aktywa, aby zapłacić odszkodowanie za szkody wynikające z naruszenia tych reguł.	

Kryteria zatwierdzenia wiążących regul korporacyjnych	W wiążących regułach korporacyjnych	W formularzu wniosku	Teksty odniesienia	Uwagi	Odniesienia do wniosku / wiążących regul korporacyjnych[6]
1.6 Ciężar dowodu spoczywa na przedsiębiorstwie, a nie na osobach fizycznych	TAK	TAK	Art. 47 ust. 2 lit. f) RODO	W wiążących regułach korporacyjnych należy stwierdzić, że na członku, którego dotyczą te reguły i który przyjął na siebie odpowiedzialność prawną, spoczywać będzie także ciężar dowodu polegający na wykazaniu, że członek, którego te reguły dotyczą i który jest zlokalizowany poza UE, nie jest odpowiedzialny za żadne naruszenie tych reguł, z powodu którego osoba, której dane dotyczą, ubiega się o odszkodowanie. Jeżeli członek, którego dotyczą wiążące reguły korporacyjne i który przyjął na siebie odpowiedzialność prawną, może udowodnić, że członek grupy spoza UE, którego dotyczą te reguły, nie jest odpowiedzialny za zdarzenie, które spowodowało szkodę, może on zostać zwolniony z ponoszenia jakiejkolwiek odpowiedzialności.	

11

Kryteria zatwierdzenia wiążących regul korporacyjnych	W wiążących regułach korporacyjnych	W formularzu wniosku	Teksty odniesienia	Uwagi	Odniesienia do wniosku / wiążących regul korporacyjnych[6]
1.7 Przejrzystość i łatwy dostęp do wiążących regul korporacyjnych dla osób, których dane dotyczą	TAK	NIE	Art. 47 ust. 2 lit. g) RODO	Wiążące reguły korporacyjne muszą zawierać zobowiązanie do przekazywania wszystkim osobom, których dane dotyczą i które korzystają z praw beneficjenta będącego osobą trzecią, informacji wymaganych w art. 13 i 14 RODO, informacji o prawach beneficjenta będącego osobą trzecią przysługujących tym osobom w zakresie przetwarzania ich danych osobowych i informacji o środkach egzekwowania tych praw, klauzuli dotyczącej odpowiedzialności prawnej i klauzul dotyczących zasad ochrony danych. Należy zapewnić wszystkie informacje – streszczenie nie wystarczy. W wiążących regułach korporacyjnych należy zawrzeć prawo każdej osoby, której dane dotyczą, do łatwego dostępu do tych reguł. W wiążących regułach korporacyjnych można przykładowo stwierdzić, że przynajmniej te części reguł, które zawierają informacje obowiązkowe dla osób, których dane dotyczą, zostaną opublikowane w internecie lub intranecie (w przypadku gdy osobami, których dane dotyczą, jest wyłącznie personel mający dostęp do intranetu).	
2 – SKUTECZNOŚĆ					
2.1 Istnienie odpowiedniego programu szkoleń	TAK	TAK	Art. 47 ust. 2 lit. n) RODO	Wiążące reguły korporacyjne muszą stanowić, że właściwe szkolenie w zakresie wiążących reguł korporacyjnych zostanie zapewnione pracownikom, którzy mają stały lub regularny dostęp do danych osobowych, uczestniczą w gromadzeniu danych lub uczestniczą	

12

Kryteria zatwierdzenia wiążących regul korporacyjnych	W wiążących regułach korporacyjnych	W formularzu wniosku	Teksty odniesienia	Uwagi	Odniesienia do wniosku / wiążących regul korporacyjnych[6]
				w opracowywaniu narzędzi wykorzystywanych do przetwarzania danych osobowych. Organy nadzorcze dokonujące oceny wiążących reguł korporacyjnych mogą zwrócić się o przedstawienie przykładów i wyjaśnień dotyczących programu szkoleniowego w toku procedury składania wniosków. Program szkoleniowy należy określić we wniosku.	
2.2 Istnienie procedury rozpatrywania skarg w zakresie wiążących regul korporacyjnych	TAK	TAK	Art. 47 ust. 2 lit. i) oraz art. 12 ust. 3 RODO	W ramach wiążących reguł korporacyjnych należy stworzyć wewnętrzny proces rozpatrywania skarg w celu zapewnienia, aby każda osoba, której dane dotyczą, mogła egzekwować swoje prawa i złożyć skargę na dowolnego członka, którego dotyczą wiążące reguły korporacyjne. - Skargami musi zająć się wydział lub osoba wyznaczeni konkretnie do tego celu, posiadający odpowiedni poziom niezależności w sprawowaniu swoich funkcji, bez zbędnej zwłoki, lecz nie później niż w terminie jednego miesiąca. Ten jednomiesięczny termin można przedłużyć maksymalnie o kolejne dwa miesiące z uwagi na skomplikowany charakter wniosku lub liczbę wniosków, w którym to przypadku należy o tym odpowiednio poinformować osobę, której dane dotyczą. W formularzu wniosku należy wyjaśnić, w jaki sposób osoby, których dane dotyczą, zostaną poinformowane o praktycznych krokach w ramach systemu składnia skarg, a w szczególności: - gdzie należy złożyć skargę;	

Kryteria zatwierdzenia wiążących regul korporacyjnych	W wiążących regułach korporacyjnych	W formularzu wniosku	Teksty odniesienia	Uwagi	Odniesienia do wniosku / wiążących regul korporacyjnych[6]
				- w jakiej formie; - o terminach udzielenia odpowiedzi na skargę; - o konsekwencjach w przypadku odrzucenia skargi; - o konsekwencjach w przypadku uznania skargi za uzasadnioną; - o konsekwencjach w przypadku, gdy osoba, której dane dotyczą, jest nieusatysfakcjonowana odpowiedzią (prawo do wniesienia skargi do sądu / organu nadzorczego).	
2.3 Istnienie programu audytu obejmującego wiążące reguły korporacyjne	TAK	TAK	Art. 47 ust. 2 lit. j) oraz art. 38 ust. 3 RODO	Wiążące reguły korporacyjne muszą nakładać na grupę obowiązek regularnego przeprowadzania audytów ochrony danych (przez wewnętrznych albo zewnętrznych akredytowanych audytorów) lub na szczególny wniosek urzędnika do spraw ochrony prywatności / osoby zajmującej się ochroną prywatności (lub jakiejkolwiek innej osoby sprawującej właściwą funkcję w organizacji) w celu zapewnienia weryfikacji zgodności z wiążącymi regułami korporacyjnymi. Wiążące reguły korporacyjne muszą stanowić, że program audytu obejmuje wszystkie aspekty wiążących reguł korporacyjnych, w tym metody zapewniania, aby przeprowadzone zostały działania naprawcze. Ponadto wiążące reguły korporacyjne muszą stanowić, że wyniki takiej weryfikacji zostaną przekazane urzędnikowi do spraw ochrony prywatności / osobie zajmującej się ochroną prywatności oraz odpowiedniemu zarządowi przedsiębiorstwa sprawującego	

Kryteria zatwierdzenia wiążących regul korporacyjnych	W wiążących regułach korporacyjnych	W formularzu wniosku	Teksty odniesienia	Uwagi	Odniesienia do wniosku / wiążących regul korporacyjnych[6]
				kontrolę w grupie przedsiębiorstw lub organowi kierującemu grupą przedsiębiorców prowadzących wspólną działalność gospodarczą. W stosownych przypadkach wyniki mogą być podane do wiadomości zarządu spółki dominującej najwyższego szczebla. Wiążące reguły korporacyjne muszą również stanowić, że organy nadzorcze mogą uzyskać dostęp do wyników audytu na wniosek, oraz nadawać organowi nadzorczemu uprawnienia do przeprowadzenia audytu w zakresie ochrony danych dowolnego członka, którego dotyczą wiążące reguły korporacyjne, o ile jest to konieczne. Formularz wniosku zawiera opis systemu audytowego. Opis ten przedstawia przykładowo następujące informacje: - który podmiot (wydział w grupie) decyduje o planie/programie audytu; - który podmiot będzie przeprowadzał audyt; - termin przeprowadzania audytu (regularnie czy na szczególny wniosek odpowiedniego pracownika ds. ochrony prywatności); - zakres audytu (np. aplikacje, systemy IT, bazy danych przetwarzające dane osobowe, dalsze przekazywanie danych, decyzje podejmowane w odniesieniu do obowiązkowego wymogu regulowanego w prawie krajowym, który jest niezgodny z wiążącymi regułami korporacyjnymi, przegląd warunków umownych stosowanych w odniesieniu do przekazywania danych	

Kryteria zatwierdzenia wiążących regul korporacyjnych	W wiążących regułach korporacyjnych	W formularzu wniosku	Teksty odniesienia	Uwagi	Odniesienia do wniosku / wiążących regul korporacyjnych[6]
				poza grupę (do administratorów lub podmiotów przetwarzających dane), działania naprawcze itd.); - który podmiot otrzyma wyniki audytów.	
2.4 Utworzenie sieci inspektorów ochrony danych (DPO) lub wyznaczenie odpowiednich pracowników w celu monitorowania przestrzegania regul	TAK	NIE	Art. 47 ust. 2 lit. h) oraz art. 38 ust. 3 RODO	Zobowiązanie do wyznaczenia DPO, jeżeli jest to wymagane na mocy art. 37 RODO, lub dowolnej innej osoby bądź dowolnego innego podmiotu (takiego jak główny urzędnik ds. ochrony prywatności) odpowiedzialnych za monitorowanie przestrzegania wiążących reguł korporacyjnych i korzystających ze wsparcia najwyższego kierownictwa podczas pełnienia tej funkcji. W pełnieniu tej funkcji DPO lub pozostałym osobom zawodowo zajmującym się kwestiami związanymi z ochroną prywatnością może – w stosownych przypadkach – pomagać zespół, sieć lokalnych DPO lub lokalnych punktów kontaktowych. DPO bezpośrednio podlega najwyższemu kierownictwu (art. 38 ust. 3 RODO). Wiążące reguły korporacyjne powinny zawierać krótki opis struktury wewnętrznej, roli, pozycji i obowiązków DPO lub osób na podobnym stanowisku oraz sieci utworzonych w celu zapewnienia przestrzegania reguł. Opis ten zawiera na przykład informacje, że DPO lub główny urzędnik ds. ochrony prywatności informuje najwyższe kierownictwo i doradza mu, zajmuje się postępowaniami prowadzonymi	

Kryteria zatwierdzenia wiążących reguł korporacyjnych	W wiążących regułach korporacyjnych	W formularzu wniosku	Teksty odniesienia	Uwagi	Odniesienia do wniosku / wiążących reguł korporacyjnych[6]
				przez organy nadzorcze, monitoruje przestrzeganie reguł na szczeblu ogólnym oraz składa na ten temat roczne sprawozdania, a także że lokalny DPO lub lokalne punkty kontaktowe mogą mieć obowiązek rozpatrywania lokalnych skarg złożonych przez osoby, których dane dotyczą, zgłaszania DPO istotnych kwestii dotyczących ochrony prywatności, monitorowania szkoleń oraz przestrzegania reguł na szczeblu lokalnym.	
3 – OBOWIĄZEK WSPÓŁPRACY					
3.1 Obowiązek współpracy z organami nadzorczymi	TAK	TAK	Art. 47 ust. 2 lit. l) RODO	Wiążące reguły korporacyjne powinny nakładać na wszystkich członków, których one dotyczą, wyraźny obowiązek współpracy z organami nadzorczymi oraz wyrażenia zgody na przeprowadzenie audytu przez te organy nadzorcze, a także zastosowania się do porad tych organów nadzorczych dotyczących wszelkich kwestii związanych z przedmiotowymi regułami.	
4 – OPIS PRZETWARZANIA I PRZEPŁYWU DANYCH					
4.1 Opis materialnego zakresu stosowania wiążących reguł korporacyjnych (charakteru przekazywanych danych, rodzaju osób lub państw, których dane dotyczą)	TAK	TAK	Art. 47 ust. 2 lit. b) RODO	W wiążących regułach korporacyjnych należy określić ich materialny zakres stosowania, a zatem muszą one zawierać ogólny opis przekazywania danych w celu umożliwienia organom nadzorczym przeprowadzenia oceny, czy przetwarzanie prowadzone w państwach trzecich jest zgodne regułami. W wiążących regułach korporacyjnych należy w szczególności określić jednorazowe lub wielokrotne przekazanie danych, w tym kategorie danych osobowych, rodzaj przetwarzania i jego cele, rodzaje osób, których dane dotyczą (dane dotyczące pracowników, klientów, dostawców	

Kryteria zatwierdzenia wiążących reguł korporacyjnych	W wiążących regułach korporacyjnych	W formularzu wniosku	Teksty odniesienia	Uwagi	Odniesienia do wniosku / wiążących reguł korporacyjnych[6]
				i innych osób trzecich przekazywane w ramach normalnej działalności gospodarczej), a także nazwę danego państwa trzeciego lub danych państw trzecich.	
4.2 Oświadczenie dotyczące zakresu geograficznego wiążących reguł korporacyjnych	TAK	TAK	Art. 47 ust. 2 lit. a) RODO	W wiążących regułach korporacyjnych określa się strukturę i dane kontaktowe odnośnej grupy przedsiębiorstw lub grupy przedsiębiorców prowadzących wspólną działalność gospodarczą i każdego z jej członków. W wiążących regułach korporacyjnych należy wskazać, czy mają zastosowanie do: (i) wszystkich danych osobowych przekazywanych z Unii Europejskiej wewnątrz grupy LUB; (ii) wszelkiego przetwarzania danych osobowych wewnątrz grupy.	
5 – MECHANIZMY ZGŁASZANIA I REJESTROWANIA ZMIAN					
5.1 Proces aktualizacji wiążących reguł korporacyjnych	TAK	TAK	Art. 47 ust. 2 lit. k) RODO	Wiążące reguły korporacyjne można modyfikować (*na przykład w celu uwzględnienia zmian w otoczeniu regulacyjnym lub strukturze przedsiębiorstwa*), powinny one jednak nakładać obowiązek bezzwłocznego informowania o zmianach wszystkich członków, których dotyczą wiążące reguły korporacyjne, oraz odpowiednich organów nadzorczych – za pośrednictwem właściwego organu nadzorczego. Aktualizacje wiążących reguł korporacyjnych lub wykazu członków, których dotyczą wiążące reguły korporacyjne, są możliwe bez konieczności ponownego składania wniosku,	

Kryteria zatwierdzenia wiążących reguł korporacyjnych	W wiążących regułach korporacyjnych	W formularzu wniosku	Teksty odniesienia	Uwagi	Odniesienia do wniosku / wiążących reguł korporacyjnych[6]
				o ile spełnione są następujące warunki: i) wyznaczona osoba lub wyznaczony zespół/dział prowadzi w pełni zaktualizowany wykaz członków, których dotyczą wiążące reguły korporacyjne, oraz monitoruje i rejestruje wszelkie aktualizacje reguł oraz – na ich wniosek – przekazuje potrzebne informacje osobom, których dane dotyczą, lub organom nadzorczym; ii) nowemu członkowi, którego dotyczą wiążące reguły korporacyjne, nie przekazuje się żadnych danych, dopóki nie będzie on w sposób skuteczny podlegał wiążącym regułom korporacyjnym i nie zapewni zgodności z tymi regułami; iii) informacje o wszelkich zmianach w wiążących regułach korporacyjnych lub w wykazie członków, których dotyczą wiążące reguły korporacyjne, powinny być przekazywane raz w roku odpowiednim organom nadzorczym za pośrednictwem właściwego organu nadzorczego, wraz z krótkim wyjaśnieniem powodów uzasadniających daną aktualizację; iv) jeżeli zmiana mogłaby wpłynąć na poziom ochrony zapewniony przez wiążące reguły korporacyjne lub znacznie wpłynąć na wiążące reguły korporacyjne (tj. zmienić ich wiążący charakter), należy o niej bezzwłocznie powiadomić odpowiednie organy nadzorcze za pośrednictwem właściwego organu nadzorczego.	
6 – ZABEZPIECZENIA					

Kryteria zatwierdzenia wiążących reguł korporacyjnych	W wiążących regułach korporacyjnych	W formularzu wniosku	Teksty odniesienia	Uwagi	Odniesienia do wniosku / wiążących reguł korporacyjnych[6]
SŁUŻĄCE OCHRONIE DANYCH					
6.1.1 Opis zasad ochrony danych, w tym reguł dotyczących przekazywania lub dalszego przekazywania danych poza terytorium UE	TAK	TAK	Art. 47 ust. 2 lit. d) RODO	Wiążące reguły korporacyjne powinny wyraźnie uwzględniać następujące zasady, których musi przestrzegać przedsiębiorstwo. Są to: i. przejrzystość, rzetelność i zgodność z prawem (art. 5 ust. 1 lit. a) oraz art. 6, 9, 10, 13 i 14 RODO); ii. ograniczenie celu (art. 5 ust. 1 lit. b) RODO); iii. minimalizacja danych i prawidłowość (art. 5 ust. 1 lit. c) i d) RODO); iv. ograniczone okresy przechowywania (art. 5 ust. 1 lit. e) RODO); v. przetwarzanie szczególnych kategorii danych osobowych; vi. bezpieczeństwo (art. 5 ust. 1 lit. f) oraz art. 32), w tym obowiązek zawierania ze wszystkimi wewnętrznymi i zewnętrznymi wykonawcami / podmiotami przetwarzającymi umów, które obejmują wszystkie wymogi określone w art. 28 ust. 3 RODO, jak również obowiązek bezzwłocznego zgłaszania wszelkich naruszeń ochrony danych osobowych siedzibie głównej w UE lub członkowi z UE, którego dotyczą wiążące reguły korporacyjne i na którego nałożono obowiązki w zakresie ochrony danych, oraz pozostałym odpowiednim urzędnikom/pracownikom ds. ochrony prywatności oraz osobom, których dane dotyczą, jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności tych	

Kryteria zatwierdzenia wiążących reguł korporacyjnych	W wiążących regułach korporacyjnych	W formularzu wniosku	Teksty odniesienia	Uwagi	Odniesienia do wniosku / wiążących reguł korporacyjnych[6]
				osób. Należy ponadto udokumentować wszelkie naruszenia ochrony danych osobowych (w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze) i należy tę dokumentację udostępnić na żądanie organu nadzorczego (art. 33 i 34 RODO); ii. ograniczenie przekazywania lub dalszego przekazywania danych podmiotom przetwarzającym i administratorom, którzy nie należą do grupy (członkowie, których dotyczą wiążące reguły korporacyjne i którzy są administratorami, mogą przekazywać dane podmiotom przetwarzającym / administratorom znajdującym się poza grupą i zlokalizowanym poza UE, jeżeli zapewniono właściwy poziom ochrony zgodnie z art. 45, 46, 47, 48 RODO lub jeżeli zgodnie z art. 49 RODO ma zastosowanie odstępstwo). Brzmienie i definicje kluczowych zasad zawartych w wiążących regułach korporacyjnych powinny być spójne z brzmieniem i definicjami w RODO.	
6.1.2 Rozliczalność i inne narzędzia	TAK	TAK	Art. 47 ust. 2 lit. d) i art. 30 RODO	Każdy podmiot działający w charakterze administratora danych jest odpowiedzialny za przestrzeganie wiążących reguł korporacyjnych i musi być w stanie wykazać ich przestrzeganie (art. 5 ust. 2 i art. 24 RODO). Aby wykazać przestrzeganie reguł, członkowie, których dotyczą wiążące reguły korporacyjne, muszą prowadzić rejestr wszystkich kategorii	

Kryteria zatwierdzenia wiążących reguł korporacyjnych	W wiążących regułach korporacyjnych	W formularzu wniosku	Teksty odniesienia	Uwagi	Odniesienia do wniosku / wiążących reguł korporacyjnych[6]
				czynności przetwarzania dokonywanych zgodnie z wymogami określonymi w art. 30 ust. 1 RODO. Rejestr ten należy prowadzić w formie pisemnej, w tym formie elektronicznej, oraz udostępniać na żądanie organu nadzorczego. Aby poprawić przestrzeganie reguł oraz gdy jest to wymagane, należy przeprowadzać oceny skutków w zakresie ochrony danych w odniesieniu do operacji przetwarzania, które z dużym prawdopodobieństwem mogą powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych (art. 35 RODO). Jeżeli ocena skutków dla ochrony danych, o której mowa w art. 35, wskaże, że przetwarzanie powodowałoby wysokie ryzyko, gdyby administrator nie zastosował środków w celu zminimalizowania tego ryzyka, należy przed rozpoczęciem przetwarzania skonsultować się z właściwym organem nadzorczym (art. 36 RODO). Należy zastosować właściwe środki techniczne i organizacyjne opracowane w celu wdrożenia zasad ochrony danych oraz ułatwienia przestrzegania w praktyce wymogów ustanowionych w wiążących regułach korporacyjnych (uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych (art. 25 RODO)).	
6.2 Wykaz podmiotów związanych wiążącymi regułami korporacyjnymi	TAK	TAK	Art. 47 ust. 2 lit. a) RODO	Wiążące reguły korporacyjne zawierają wykaz podmiotów związanych tymi regułami, w tym ich dane kontaktowe.	

Kryteria zatwierdzenia wiążących regul korporacyjnych	W wiążących regułach korporacyjnych	W formularzu wniosku	Teksty odniesienia	Uwagi	Odniesienia do wniosku / wiążących regul korporacyjnych[6]
6.3 Potrzeba zachowania przejrzystości w przypadkach, w których przepisy krajowe uniemożliwiają grupie przestrzeganie wiążących regul korporacyjnych	TAK	NIE	Art. 47 ust. 2 lit. m) RODO	Wyraźne zobowiązanie, że w przypadkach, gdy członek, którego dotyczą wiążące reguły korporacyjne, ma powody, by sądzić, iż mające do niego zastosowanie przepisy uniemożliwiają mu wywiązanie się z obowiązków wynikających z wiążących reguł korporacyjnych lub mają istotny wpływ na udzielane w ramach tych reguł gwarancje, powiadomi on niezwłocznie o tym fakcie siedzibę główną w UE lub członka z UE, którego dotyczą wiążące reguły korporacyjne i na którego nałożono obowiązki w zakresie ochrony danych, oraz pozostałych odpowiednich urzędników/pracowników ds. ochrony prywatności (o ile organ ścigania nie wydał zakazu na mocy prawa karnego np. w celu zachowania poufności postępowania prowadzonego przez organy ścigania). Wiążące reguły korporacyjne powinny ponadto zawierać zobowiązanie do tego, aby w przypadku gdy jakikolwiek wymóg prawny, któremu podlega w państwie trzecim członek, którego dotyczą wiążące reguły korporacyjne, może mieć istotny niekorzystny wpływ na gwarancje przewidziane w wiążących regułach korporacyjnych – należy zgłosić ten problem właściwemu organowi nadzorczemu. Obejmuje to wszelkie prawnie wiążące wnioski o ujawnienie danych osobowych ze strony organów ścigania lub organu ds. bezpieczeństwa państwa. W takim przypadku należy odpowiednio poinformować o wniosku właściwy organ nadzorczy, w tym należy przekazać mu informacje na temat danych będących przedmiotem wniosku, podmiotu składającego wniosek i podstawy prawnej	

Kryteria zatwierdzenia wiążących regul korporacyjnych	W wiążących regułach korporacyjnych	W formularzu wniosku	Teksty odniesienia	Uwagi	Odniesienia do wniosku / wiążących regul korporacyjnych[6]
				ujawnienia (chyba że wydano zakaz takiego powiadomienia, na przykład na mocy prawa karnego w celu zachowania poufności postępowań prowadzonych przez organy ścigania). Jeżeli w szczególnych przypadkach zawieszenie lub powiadomienie są zakazane, wiążące reguły korporacyjne stanowią, że członek, którego dotyczą wiążące reguły korporacyjne i do którego zwrócono się z wnioskiem, dołoży wszelkich starań w celu uzyskania prawa uchylenia tego zakazu, aby przekazać możliwie największą ilość informacji w możliwie najkrótszym terminie i być w stanie wykazać, że je przekazał. Jeżeli w powyższych przypadkach – pomimo dołożenia wszelkich starań – członek, którego dotyczą wiążące reguły korporacyjne i do którego zwrócono się z wnioskiem, nie jest w stanie powiadomić właściwych organów nadzorczych, musi zobowiązać się w wiążących regułach korporacyjnych do przekazywania corocznie do właściwych organów nadzorczych ogólnych informacji na temat otrzymanych wniosków (np. dotyczących liczby wniosków o ujawnienie, rodzaju danych będących przedmiotem wniosków, w miarę możliwości – osoby składającej wniosek itd.). W każdym razie wiążące reguły korporacyjne muszą stanowić, że przekazywanie danych osobowych przez członka grupy, którego dotyczą wiążące reguły korporacyjne,	

Kryteria zatwierdzenia wiążących reguł korporacyjnych	W wiążących regułach korporacyjnych	W formularzu wniosku	Teksty odniesienia	Uwagi	Odniesienia do wniosku / wiążących reguł korporacyjnych[6]
				dowolnemu organowi publicznemu, nie może być masowe, nieproporcjonalne i powszechne w sposób, który wykraczałby poza to, co jest konieczne w demokratycznym społeczeństwie.	
6.4 Oświadczenie dotyczące relacji między prawem krajowym a wiążącymi regułami korporacyjnymi	TAK	NIE	Nie dotyczy	W wiążących regułach korporacyjnych określa się relacje między wiążącymi regułami korporacyjnymi a odpowiednim prawem właściwym. Wiążące reguły korporacyjne stanowią, że w sytuacji, gdy zgodnie z prawodawstwem miejscowym, na przykład prawodawstwem UE, wymaga się wyższego poziomu ochrony danych osobowych, wówczas będzie ono nadrzędne wobec wiążących reguł korporacyjnych. W każdym przypadku dane osobowe przetwarzane są zgodnie z prawem właściwym, jak przewidziano w art. 5 RODO i odpowiednich przepisach miejscowych.	

25

26

ARTICLE 29 DATA PROTECTION WORKING PARTY

18/EN
WP 257 rev.01

Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules

Adopted on 28 November 2017
As last Revised and Adopted on 6 February 2018

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.
The secretariat is provided by Directorate C (Fundamental Rights and Union Citizenship) of the European Commission, Directorate General Justice, B-1049 Brussels, Belgium, Office No MO-59 02/013.
Website: http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358&tpa_id=6936

INTRODUCTION

In order to facilitate the use of Binding Corporate Rules for Processors (BCR-P) by a corporate group or a group of enterprises engaged in a joint economic activity for international transfers from organisations established in the EU to organisations within the same group established outside the EU, the Article 29 Working Party (WP29) has amended the Working Document 195 (which was adopted in 2012) setting up a table with the elements and principles to be found in Binding Corporate Rules in order to reflect the requirements referring to BCRs now expressly set out in Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation / GDPR).

It should be recalled that BCR-P apply to data received from a controller established in the EU which is not a member of the group and then processed by the group members as processors and/or sub processors; whereas BCRs for Controllers (BCR-C) are suitable for framing transfers of personal data from controllers established in the EU to other controllers or to processors established outside the EU within the same group. Hence the obligations set out in the BCR-P apply in relation to third party personal data that are processed by a member of the group as a processor according to the instructions from a non-group controller.

According to Article 28.3 of the GDPR, a contract or another legal act under Union or Member State law that is binding on the processor with regard to the controller must be implemented between the controller and the processor. Such a contract or other legal act will be referred here as the "service agreement"..

Taking into account that Article 47.2 of the GDPR lists a minimum set of elements to be contained within a BCR, this amended table is meant to:

- Adjust the wording of the previous referential so as to bring it in line with Article 47 GDPR,
- Clarify the necessary content of a BCR as stated in Article 47 and in document WP 204[1] adopted by the WP29 within the framework of the Directive 95/46/EC,
- Make the distinction between what must be included in BCRs and what must be presented to the competent Supervisory Authority in the BCRs application (document WP 195a[2]), and
- Provide explanations/comments on each of the requirements.

Article 47 of the GDPR is clearly modelled on the Working documents relating to BCRs adopted by the WP29. However, it specifies some new elements that need to be taken into account when updating already existing approved BCRs or adopting new sets of BCRs so as to ensure their compatibility with the new framework established by the GDPR.

1. New elements

[1] Working Document WP204: Explanatory Document on the Processor Binding Corporate Rules, as last revised and adopted on 22 May 2015
[2] Working Document WP 195a: Recommendation 1/2012 on the Standard Application form for Approval of Binding Corporate Rules for the Transfer of Personal Data for Processing Activities, adopted on 17 September 2012

In this perspective, the WP29 would like to draw attention in particular to the following elements:

- ***Scope of application***: The BCRs shall specify the structure and contact details of the group of undertakings or group of enterprises engaged in a joint economic activity and of each of its members (Art. 47.2.a GDPR). The BCRs must also provide its material scope, for instance the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the types of data subjects affected and the identification of the third country or countries (Art. 47.2.b GDPR);

- ***Third party beneficiary rights***: Data subjects should be able to enforce the BCRs as third party beneficiaries directly against the processor where the requirements at stake are specifically directed to processors in accordance with the GDPR (Art. 28, 29, 79 GDPR);

- ***Right to lodge a complaint***: Data subjects should be given the right to bring their claim, at their choice, either before the Supervisory Authority ('SA') in the Member State of his habitual residence, place of work or place of the alleged infringement (Art.77 GDPR) or before the competent court of the EU Member States (choice for the data subject to act before the courts where the data exporter has an establishment or where the data subject has his or her habitual residence (Article 79 GDPR);

- ***Data Protection principles***: Along with the obligations arising from principles of transparency, fairness, lawfulness, purpose limitation, data quality, security, the BCRs should also explain how other requirements, such as, in particular, in relation to data subjects rights, sub-processing and onward transfers to entities not bound by the BCRs will be observed by the processor;

- ***Accountability***: Processors will have an obligation to make available to the controller all information necessary to demonstrate compliance with their obligations including through audits and inspections conducted by the Controller or an auditor mandated by the Controller (Art. 28-3-h GDPR);

- ***Service Agreement***: The Service Agreement between the Controller and the Processor must contain all required elements as provided by Article 28 of the GDPR.

2. Amendments of already adopted BCRs

While in accordance with article 46-5 of the GDPR, authorisations by a Member State or supervisory authority made on the basis of Article 26(2) of Directive 95/46/EC will remain valid until amended, replaced or repealed, if necessary, by that supervisory authority, groups with approved BCRs should, in preparing to the GDPR, bring their BCRs in line with GDPR requirements.

This document aims also to assist those groups with approved BCRs in implementing the relevant changes to bring them in line with the GDPR. To this end, these groups are invited to notify the relevant changes to their BCRs as part of their obligation (under 5.1 of WP195) to all group members and to the DPAs via the Lead DPA under their annual update as of 25 May 2018. Such updated BCRs can be used without having to apply for a new authorization or approval from the DPAs.

Taking into account the above, the DPAs reserve their right to exercise their powers under article 46-5 of the GDPR.

Criteria for approval of BCRs	In the BCRs	In the application form	Comments	References to Application/BCRs
1 - BINDING NATURE				
INTERNALLY				
1.1 The duty to respect the BCRs	YES	YES	The BCRs must be legally binding and shall contain a clear duty for each participating member of the Group of undertakings or group of enterprises engaged in a joint economic activity ("BCR member") including their employees to respect the BCRs. The BCRs shall also expressly state that each Member including their employees shall respect the instructions from the controller regarding the data processing and the security and confidentiality measures as provided in the Service Agreement (Art. 28, 29 and 32 of the GDPR).	
1.2 An explanation of how the rules are made binding on the members of the group and also the employees	NO	YES	The Group will have to explain in its application form how the rules are made binding : i) For each BCR member by one or more of: - Intra-group agreement, - Unilateral undertakings (this is only possible if the BCR member taking responsibility and liability is located in a Member State that recognizes Unilateral undertakings as binding and if this BCR member is legally able to bind the other BCR members), or - Other means (only if the group demonstrates how bindingness is achieved). ii) On employees by one or more of: - Individual and separate agreement/undertaking with sanctions, or Clause in employment contract with sanctions, or - Internal policies with sanctions, or - Collective agreements with sanctions, or - Other means (but the group must properly explain how the BCRs are made binding on the employees).	

Criteria for approval of BCRs	In the BCRs	In the application form	Comments	References to Application/BCRs
EXTERNALLY				
1.3 The creation of third-party beneficiary rights for data subjects, including the possibility to lodge a complaint before the competent Supervisory Authorities and before the Courts	YES	YES	i) Rights which are directly enforceable against the processor The BCRs must grant rights to data subjects to enforce the BCRs as third party beneficiaries directly against the processor where the requirements at stake are specifically directed to processors in accordance with the GDPR. In this regard, data subjects shall at least be able to enforce the following elements of the BCRs directly against the processor: - Duty to respect the instructions from the controller regarding the data processing including for data transfers to third countries (Art. 28.3.a, 28.3.g., 29 GDPR and section 1.1, 6.1.ii and 6.1.iv of this referential), - Duty to implement appropriate technical and organizational security measures (Art. 28.3.c and 32 GDPR and section 6.1.iv of this referential) and duty to notify any personal data breach to the controller (Art. 33.2 GDPR and section 6.1.iv of this referential), - Duty to respect the conditions when engaging a sub-processor either within or outside the Group (Art. 28.2, 28.3.d . 28.4, 45, 46, 47 GDPR, section 6.1.vi and 6.1.vii of this referential), Duty to cooperate with and assist the controller in complying and demonstrating compliance with the law such as for answering requests from data subjects in relation to their rights (Art. 28.3.e, 28.3.f, 28.3.h and sections 3.2, 6.1.i, 6.1.iii, 6.1.iv, 6.1. v and 6.1. 2 of this referential) - Easy access to BCRs (Art.47.2.g GDPR and section 1.8 of this referential) - Right to complain through internal complaint mechanisms (Art.47.2.i and section 2.2 of this referential).	

Criteria for approval of BCRs	In the BCRs	In the application form	Comments	References to Application/BCRs
			- Duty to cooperate with the supervisory authority (Art. 31, 47.2.l of GDPR and section 3.1 of this referential) - Liability, compensation and jurisdiction provisions (Art.47.2.e, 79, 82 GDPR and sections 1.3, 1.5 and 1.7 of this referential). - National legislation preventing respect of BCRs (Art.47.2.m and section 6.3 of this referential) ii) Rights which are enforceable against the processor in case the data subject is not able to bring a claim against the controller : The BCRs must expressly confer rights to data subjects to enforce the BCRs as third-party beneficiaries in case the data subject is not able to bring a claim against the data controller; because the data controller has factually disappeared or ceased to exist in law or has become insolvent, unless any successor entity has assumed the entire legal obligations of the data controller by contract of by operation of law, in which case the data subject can enforce its rights against such entity. In such a case, data subjects shall at least be able to enforce against the processor the following sections set out in this referential: 1.1, 1.3, 1.5, 1.7, 1.8, 2.2, 3.1, 3.2, 6.1, 6.2, 6.3 The data subjects' rights as mentioned under i) and ii) shall cover the judicial remedies for any breach of the third party beneficiary rights guaranteed and the right to obtain redress and where appropriate receive compensation for any damage (material harm but also any distress). In particular, data subjects shall be entitled to lodge a complaint before the competent supervisory authority (choice between the supervisory authority of the EU Member State of his/her habitual residence, place of work or place of alleged infringement) and before the competent court of the EU Member State (choice for the data subject to act before the courts where the controller or processor has an establishment or where the data subject has his or her habitual residence pursuant to Article 79 of the	

Criteria for approval of BCRs	In the BCRs	In the application form	Comments	References to Application/BCRs
			GDPR). Where the processor and the controller involved in the same processing are found responsible for any damage caused by such processing, the data subject shall be entitled to receive compensation for the entire damage directly from the processor (Art. 82.4 GDPR)	
1.4. Responsibility towards the Controller	YES	YES	The BCRs shall be made binding towards the Controller through a specific reference to it in the Service Agreement which shall comply with art 28 of the GDPR. Moreover, the BCR must state that the Controller shall have the right to enforce the BCR against any BCR member for breaches they caused, and, moreover, against the BCR member referred under point 1.5 in case of a breach of the BCRs or of the Service Agreement by BCR members established outside of EU or of a breach of the written agreement referred under 6.1.vii, by any external sub-processor established outside of the EU.	

Criteria for approval of BCRs	In the BCRs	In the application form	Comments	References to Application/BCRs
1.5 The company accepts liability for paying compensation and to remedy breaches of the BCRs.	YES	YES	The BCRs must contain a duty for the EU headquarters of the Processor or the EU BCR member of the Processor with delegated data protection responsibilities or the EU exporter Processor (e.g. the EU party contracting with the controller) to accept responsibility for and to agree to take the necessary action to remedy the acts of other BCR members established outside of EU or breaches caused by external sub-processor established outside of EU and to pay compensation for any damages resulting from a violation of the BCRs. This BCR member will accept liability as if the violation had taken place by him in the Member State in which he is based instead of the BCR member outside the EU or the external sub-processor established outside of EU. This BCR member may not rely on a breach by a sub-processor (internal or external of the group) of its obligations in order to avoid its own liabilities. If it is not possible for some groups with particular corporate structures to impose all the responsibility for any type of breach of the BCRs outside of the EU on a specific entity, another option may consist of stating that each and every BCR member exporting data out of the EU will be liable for any breaches of the BCR by the sub-processors (internal or external of the group) established outside the EU which received the data from this EU BCR member.	
1.6 The company has sufficient assets.	NO	YES	The application form must contain a confirmation that any BCR member that has accepted liability for the acts of other BCR members outside of EU and/or for any external sub-processor established outside of EU has sufficient assets to pay compensation for damages resulting from the breach of the BCRs.	
1.7 The burden of proof lies with the company not the individual.	YES	YES	The BCRs must state that the BCR member that has accepted liability will have the burden of proof to demonstrate that the BCR member outside the EU or the external sub-processor is not liable for any violation of the rules which has resulted in the data subject claiming damages The BCRs must also state that where the Controller can demonstrate that	

Criteria for approval of BCRs	In the BCRs	In the application form	Comments	References to Application/BCRs
			it suffered damage and establish facts which show it is likely that the damage has occurred because of the breach of BCRs, it will be for the BCR member of the group that accepted liability to prove that the BCR member outside of the EU or the external sub-processor was not responsible for the breach of the BCRs giving rise to those damages or that no such breach took place If the entity that has accepted liability can prove that the BCR member outside the EU is not responsible for the act, it may discharge itself from any responsibility/liability.	
1.8 There is easy access to BCRs for data subjects and in particular easy access to the information about third party beneficiary rights for the data subject that benefit from them.	YES	NO	Access for the Controller: The Service Agreement will ensure that the BCRs are part of the contract. BCRs will be annexed to the Service Agreement or a reference to it will be made with a possibility of electronic access. Access for Data Subjects: BCRs must contain the commitment that all data subjects benefiting from the third party beneficiary rights should, in particular, be provided with the information on their third party beneficiary rights with regard to the processing of their personal data and on the means to exercise those rights. The BCRs must stipulate the right for every data subject to have easy access to them. Relevant parts of the BCRs shall be published on the website of the Processor Group or other appropriate means in a way easily accessible to data subjects or at least a document including **all** (and not a summary of) the information relating to points 1.1, 1.3, 1.4, 1.6, 1.7, 2.2, 3.1, 3.2, 4.1, 4.2, 6.1, 6.2, 6.3 of this referential.	
2 – EFFECTIVENESS				
2.1 The existence of a suitable training programme	YES	YES	The BCRs must state that appropriate training on the BCRs will be provided to personnel that have permanent or regular access to personal data who are involved in the collection of personal data or in the development of tools used to process personal data. The Supervisory Authorities evaluating the BCRs may ask for some examples and explanation of the training programme during the application procedure and the training programme shall be specified in the application.	

Criteria for approval of BCRs	In the BCRs	In the application form	Comments	References to Application/BCRs
2.2 The existence of a complaint handling process for the BCRs	YES	YES	The BCRs shall contain a commitment from the Processor Group to create a specific contact point for data subjects. All BCR members shall have the duty to communicate a claim or request without undue delay to the Controller without obligation to handle it, (except if it has been agreed otherwise with the Controller). The BCRs shall contain a commitment for the Processor to handle complaints from data subjects where the Controller has disappeared factually or has ceased to exist in law or became insolvent. In all cases where the processor handles complaints, these shall be dealt without undue delay and in any event within one month by a clearly identified department or person who has an appropriate level of independence in the exercise of his/her functions. Taking into account the complexity and number of the requests, that period may be extended by two further months at the utmost, in which case the data subject should be informed accordingly. The application form must explain how data subjects will be informed about the practical steps of the complaint system, in particular : - where to complain, - in what form, - delays for the reply on the complaint, - consequences in case of rejection of the complaint - consequences in case the complaint is considered as justified - consequences if the data subject is not satisfied by the replies (right to lodge a claim before the Court/Supervisory Authority)	
2.3 The existence of an audit programme covering the BCRs	YES	YES	The BCRs must create a duty for the group to have data protection audits on regular basis (by either internal or external accredited auditors) or on specific request from the privacy officer/function (or any other competent function in the organization) to ensure the verification of compliance with the BCRs. The BCRs must state that the audit programme covers all aspects of the	

Criteria for approval of BCRs	In the BCRs	In the application form	Comments	References to Application/BCRs
			BCRs including methods of ensuring that corrective actions will take place. Moreover, the BCRs must state that the result will be communicated to the privacy officer/function and to the relevant board of the controlling undertaking of a group or of the group of enterprises engaged in a joint economic activity but also will be made accessible to the Controller. Where appropriate, the result may be communicated to the ultimate parent's board. The BCRs must state that the Supervisory Authorities competent for the Controller can have access to the results of the audit upon request and give the Supervisory Authorities the authority/power to carry out a data protection audit of any BCR member if required. Any processor or sub-processor processing the personal data on behalf of a particular controller will accept, at the request of that controller, to submit their data processing facilities for audit of the processing activities relating to that controller which shall be carried out by the controller or an inspection body composed of independent members and in possession of the required professional qualifications, bound by a duty of confidentiality, selected by the data controller, where applicable, in agreement with the Supervisory Authority. The application form will contain a description of the audit system. For instance: - Which entity (department within the group) decides on the audit plan/programme, - Which entity will conduct the audit, - Time of the audit (regularly or on specific request from the appropriate Privacy function.) - Coverage of the audit (for instance, applications, IT systems, databases that process Personal Data, or onward transfers, decisions taken as regards mandatory requirement under national laws that conflicts with the BCRs, review of the contractual terms used for the transfers out of the Group (to controllers or processors of data), corrective actions, …) - Which entity will receive the results of the audits.	

Criteria for approval of BCRs	In the BCRs	In the application form	Comments	References to Application/BCRs
2.4 The creation of a network of data protection officers (DPO) or appropriate staff for monitoring compliance with the rules	YES	NO	A commitment to appoint a DPO where required in line with article 37 of the GDPR or any other person or entity (such as a chief privacy officer) with responsibility to monitor compliance with the BCRs. This person/entity shall enjoy the highest management support in exercising this function. The DPO or other person/entity as mentioned, respectively, can be assisted, in exercising this function, by a team/a network of local DPOs or local contacts as appropriate. The DPO shall directly report to the highest management level (GDPR Art. 38.3). A brief description of the internal structure, role, position and tasks of the DPO or similar function, as mentioned, and the team/network created to ensure compliance with the rules. For example, that the DPO or chief Privacy Officer informs and advises the highest management, deals with Supervisory Authorities' investigations, monitors and annually reports on BCRs compliance at a global level, and that local DPOs or local contacts are in charge of reporting major privacy issues to the DPO or chief privacy officer, monitoring training and compliance at a local level.	
3 – COOPERATION DUTY				
3.1 A duty to cooperate with Supervisory Authorities	YES	YES	The BCRs shall contain a clear duty for all BCR members to cooperate with and to accept to be audited by the Supervisory Authorities competent for the relevant controller and to comply with the advice of these Supervisory Authorities on any issue related to those rules.	
3.2 A duty to cooperate with the Controller	YES	YES	The BCRs shall contain a clear duty for any processor or sub-processor to co-operate and assist the Controller to comply with data protection law (such as its duty to respect the data subject rights or to handle their complaints, or to be in a position to reply to investigation or inquiry from Supervisory Authorities). This shall be done in a reasonable time and to the extent reasonably possible.	

Criteria for approval of BCRs	In the BCRs	In the application form	Comments	References to Application/BCRs
4 – DESCRIPTION OF PROCESSING AND DATA FLOWS				
4.1 A description of the transfers and material scope covered by the BCRs	YES	YES	The BCRs shall contain a list of BCR members, i.e. entities that are bound by the BCRs (see also point 6.2) The Processor submitting a BCR shall give a general description to the Supervisory Authority of the material scope of the BCRs (expected nature of the data transferred, categories of personal data, types of data subjects concerned by the transfers, anticipated types of processing and its purposes.	
4.2 A statement of the geographical scope of the BCRs (nature of data, type of data subjects, countries)	YES	YES	The BCRs shall specify the structure and contact details of the group of undertakings or group of enterprises engaged in a joint economic activity and of each of the BCR members. The BCRs shall indicate that it is up to the Controller to apply the BCRs to: i) All personal data processed for processor activities and that are submitted to EU law (for instance, data has been transferred from the European Union), OR; ii) All processing of data processed for processor activities within the group whatever the origin of the data.	
5 - MECHANISMS FOR REPORTING AND RECORDING CHANGES				
5.1 A process for updating the BCRs	YES	YES	The BCRs can be modified (for instance to take into account modifications of the regulatory environment or the company structure) but they shall impose a duty to report changes to all BCR members, and to the relevant Supervisory Authorities, via the competent Supervisory Authorities and to the controller. Where a change affects the processing conditions, the information should be given to the controller in such a timely fashion that the controller has the possibility to object to the change or to terminate the contract before the modification is made (for instance, on any intended changes concerning the addition or replacement of subcontractors, before the data	

Criteria for approval of BCRs	In the BCRs	In the application form	Comments	References to Application/BCRs
			are communicated to the new sub-processor). Updates to the BCRs or to the list of the BCR members are possible without having to re-apply for an approval providing that: i) An identified person or team/department keeps a fully updated list of the BCR members and of the sub-processors involved in the data processing activities for the controller which shall be made accessible to the data controller, data subject and Supervisory Authorities. ii) This person will keep track of and record any updates to the rules and provide the necessary information systematically to the data controller and upon request to Supervisory Authorities upon request. iii) No transfer is made to a new BCR member until the new BCR member is effectively bound by the BCR and can deliver compliance. iv) Any changes to the BCRs or to the list of BCR members shall be reported once a year to the relevant Supervisory Authorities, via the competent Supervisory Authority with a brief explanation of the reasons justifying the update. v) Where a modification would affect the level of the protection offered by the BCRs or significantly affect the BCRs (i.e. changes in the bindingness), it must be promptly communicated to the relevant Supervisory Authorities via the competent Supervisory Authority.	
6 - DATA PROTECTION SAFEGUARDS				
6.1 A description of the privacy principles including the rules on transfers or onward transfers outside of the EU	YES	YES	The BCRs shall include the following principles to be observed by any BCR member: i) Transparency, fairness, and lawfulness: Processors and sub-processors will have a general duty to help and assist the controller to comply with the law (for instance, to be transparent about sub-processor	

Criteria for approval of BCRs	In the BCRs	In the application form	Comments	References to Application/BCRs
			activities in order to allow the controller to correctly inform the data subject); ii) Purpose limitation: duty to process the personal data only on behalf of the controller and in compliance with its documented instructions including with regard to transfers of personal data to a third country, unless required to do so by Union or Member State law to which the processor is subject. In such a case, the processor shall inform the controller of that legal requirement before processing takes place, unless that law prohibits such information on important grounds of public interest (Art. 28-3-a of the GDPR). In other cases, if the processor cannot provide such compliance for whatever reasons, it agrees to inform promptly the data controller of its inability to comply, in which case the controller is entitled to suspend the transfer of data and/or terminate the contract. On the termination of the provision of services related to the data processing, the processors and sub-processors shall, at the choice of the controller, delete or return all the personal data transferred to the controller and delete the copies thereof and certify to the controller that it has done so, unless legislation imposed upon them requires storage of the personal data transferred. In that case, the processors and the sub-processors will inform the controller and warrant that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore. iii) Data quality: Processors and sub-processors will have a general duty to help and assist the controller to comply with the law, in particular: - Processors and sub-processors will execute any necessary measures when asked by the Controller, in order to have the data updated, corrected or deleted. Processors and sub-processors will inform each BCR member to whom the data have been disclosed of any rectification, or deletion of data.	

Criteria for approval of BCRs	In the BCRs	In the application form	Comments	References to Application/BCRs
			- Processors and sub-processors will execute any necessary measures, when asked by the Controller, in order to have the data deleted or anonymised from the moment the identification form is not necessary anymore. Processor and sub-processors will communicate to each entity to whom the data have been disclosed of any deletion or anonymisation of data. iv) Security: Processors and sub-processors will have a duty to implement all appropriate technical and organizational measures to ensure a level of security appropriate to the risks presented by the processing as provided by Article 32 of the GDPR. Processors and sub-processors will also have a duty to assist the Controller in ensuring compliance with the obligations as set out in Articles 32 to 36 of the GDPR taking into account the nature of processing and information available to the processor (Art.28-3-f of the GDPR). Processors and sub-processors must implement technical and organisational measures which at least meet the requirements of the data controller's applicable law and any existing particular measures specified in the Service Agreement. Processors shall inform the Controller without undue delay after becoming aware of any personal data breach. In addition, sub-processors shall have the duty to inform the Processor and the Controller without undue delay after becoming aware of any personal data breach. v) Data subject rights: Processors and sub-processors will execute any appropriate technical and organizational measures, insofar as this is possible, when asked by the controller, for the fulfilment of the controller's obligations to respond to requests for exercising the data subjects rights as set out in Chapter III of the GDPR (Art. 28-3-e of the GDPR) including by communicating any useful information in order to help the controller to comply with the duty to respect the rights of the data subjects. Processor and sub-processors will transmit to the controller any data subject request without answering it unless he is authorised to do so.	

Criteria for approval of BCRs	In the BCRs	In the application form	Comments	References to Application/BCRs
			vi) Sub-processing within the Group: data may be sub-processed by other BCR members bound by the BCRs only with the prior informed specific or general written authorization of the controller[3]. The Service Agreement will specify if a general prior authorization given at the beginning of the service would be sufficient or if a specific authorization will be required for each new sub-processor. If a general authorization is given, the controller should be informed by the processor of any intended changes concerning the addition or replacement of a sub-processor in such a timely fashion that the controller has the possibility to object to the change or to terminate the contract before the data are communicated to the new sub-processor. vii) Onward transfers to external sub-processors: Data may sub processed by non-members of the BCRs only with the prior informed specific or general written authorization of the controller[4]. If a general authorization is given, the controller should be informed by the processor of any intended changes concerning the addition or replacement of sub-processors in such a timely fashion that the controller has the possibility to object to the change or to terminate the contract before the data are communicated to the new sub-processor. Where the BCR member bound by the BCRs subcontracts its obligations under the Service Agreement, with the authorization of the controller, it shall do so only by way of a contract or other legal act under Union or Member State law with the sub-processor which provides that adequate protection is provided as set out in Articles 28, 29, 32, 45, 46, 47 of the GDPR and which ensures that the same data protection obligations as set	

[3] Information on the main elements (parties, countries, security, guarantees in case of international transfers, with a possibility to get a copy of the contracts used). The detailed information, for instance relating to the name of the sub-processors could be provided e.g. in a public digital register.
[4] Information on the main elements (parties, countries, security, guarantees in case of international transfers, with a possibility to get a copy of the contracts used). The detailed information, for instance relating to the name of the sub-processors could be provided e.g. in a public digital register.

Criteria for approval of BCRs	In the BCRs	In the application form	Comments	References to Application/BCRs
			out in the Service Agreement between the controller and the processor and sections 1.3, 1.4, 3 and 6 of this referential are imposed on the sub-processor, in particular providing sufficient guarantees to implement appropriate technical and organization measures in such a manner that the processing will meet the requirements of the GDPR (Art. 28-4 of the GDPR).	
6.1.2 Accountability *and other tools*	YES	YES	Processors will have a duty to make available to the controller all information necessary to demonstrate compliance with their obligations as provided by Article 28-3-h of the GDPR and allow for and contribute to audits, including inspections conducted by the controller or another auditor mandated by the controller. In addition, the processor shall immediately inform the controller if in its opinion, an instruction infringes the GDPR or other Union or Member State data protection provisions. In order to demonstrate compliance with the BCRs, BCR members need to maintain a record of all categories of processing activities carried out on behalf of each controller in line with the requirements as set out in Art. 30.2 GDPR. This record should be maintained in writing, including in electronic form and should be made available to the supervisory authority on request (Art.30.3 and 30.4 GDPR) The BCR members shall also assist the controller in implementing appropriate technical and organisational measures to comply with data protection principles and facilitate compliance with the requirements set up by the BCRs in practice such as data protection by design and by default (Art. 25 and 47.2.d GDPR)	
6.2 The list of entities bound by BCRs	YES	YES	BCR shall contain a list of the entities bound by the BCRs including contact details.	
6.3 The need to be transparent where national legislation prevents the group from complying with the BCRs	YES	NO	A clear commitment that where a BCR member has reasons to believe that the existing or future legislation applicable to it may prevent it from fulfilling the instructions received from the controller or its obligations under the BCRs or Service Agreement, it will promptly notify this to the controller which is entitled to suspend the transfer of data and/or terminate the contract, to the EU headquarter processor or EU member	

Criteria for approval of BCRs	In the BCRs	In the application form	Comments	References to Application/BCRs
			with delegated data protection responsibilities or the other relevant Privacy Officer/function, but also to the Supervisory Authority competent for the controller and the Supervisory authority competent for the processor. Any legally binding request for disclosure of the personal data by a law enforcement authority or state security body shall be communicated to the controller unless otherwise prohibited (such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation). In any case, the request for disclosure should be put on hold and the Supervisory Authority competent for the controller and the competent Supervisory Authority for the processor should be clearly informed about the request, including information about the data requested, the requesting body and the legal basis for disclosure (unless otherwise prohibited). If in specific cases the suspension and/or notification are prohibited, the BCRs shall provide that the requested BCR member will use its best efforts to obtain the right to waive this prohibition in order to communicate as much information as it can and as soon as possible, and be able to demonstrate that it did so. If, in the above cases, despite having used its best efforts, the requested BCR member is not in a position to notify the competent SAs, it must commit in the BCRs to annually provide general information on the requests it received to the competent SAs (e.g. number of applications for disclosure, type of data requested, requester if possible, etc.). In any case, the BCRs must state that transfers of personal data by a BCR member of the group to any public authority cannot be massive, disproportionate and indiscriminate in a manner that would go beyond what is necessary in a democratic society	
6.4 A statement about the relationship between national laws and BCRs	YES	NO	BCRs shall specify the relationship between the BCRs and the relevant applicable law. The BCRs shall state that, where the local legislation, for instance EU	

Criteria for approval of BCRs	In the BCRs	In the application form	Comments	References to Application/BCRs
			legislation, requires a higher level of protection for personal data it will take precedence over the BCRs. In any event data shall be processed in accordance with the applicable law.	

II. COMMITMENTS TO BE TAKEN IN THE SERVICE LEVEL AGREEMENT

The BCRs for Processors shall unambiguously be linked to the Service Level Agreement signed with each Client. To that extent, it is important to make sure in the Service Level Agreement, which must contain all required elements provided by Article 28 of the GDPR, that:

- BCRs will be made enforceable for the Controller (Client) through a specific reference to it in the SLA (as an annex).
- The Controller shall commit that if the transfer involves special categories of data the Data Subject has been informed or will be informed before the transfer that his data could be transmitted to a third country not providing adequate protection;
- The Controller shall also commit to inform the data subject about the existence of processors based outside of EU and of the BCRs. The Controller shall make available to the Data Subjects upon request a copy of the BCRs and of the service agreement (without any sensitive and confidential commercial information);
- Clear confidentiality and security measures are described or referred with an electronic link;
- A clear description of the instructions and the data processing;
- The service agreement will specify if data may be sub-processed inside of the Group or outside of the group and will specify if the prior authorization to it expressed by the controller is general or needs to be given specifically for each new sub-processing activities.

GRUPA ROBOCZA ART. 29

18/PL

WP 254 rev. 01

Grupa Robocza Art. 29

Odpowiedni stopień ochrony przekazywanych danych osobowych

Przyjęty dnia 28 listopada 2017 r.

Ostatnio zmieniony i przyjęty dnia 6 lutego 2018 r.

Grupa Robocza została powołana na mocy art. 29 dyrektywy 95/46/WE. Jest ona niezależnym europejskim organem doradczym w zakresie ochrony danych i prywatności. Zadania Grupy zostały określone w przepisach art. 30 dyrektywy 95/46/WE i art. 15 dyrektywy 2002/58/WE.

Obsługę sekretariatu zapewnia Komisja Europejska, Dyrekcja C (Prawa Podstawowe i Obywatelstwo Unii Europejskiej) Dyrekcji Generalnej ds. Sprawiedliwości, B-1049 Bruksela, Belgia, biuro nr MO-59 02/013.

Strona internetowa: http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358&tpa_id=6936

Wprowadzenie

Grupa robocza organów ochrony danych UE[1] (Grupa Robocza Art. 29) opublikowała uprzednio dokument roboczy w sprawie przekazywania danych osobowych do państw trzecich (WP12)[2]. Wraz z zastąpieniem dyrektywy unijnym ogólnym rozporządzeniem o ochronie danych (RODO)[3] Grupa Robocza Art. 29 dokonała przeglądu dokumentu roboczego WP12, stanowiącego jej wcześniejsze wytyczne, aby zaktualizować go w kontekście nowych przepisów i najnowszego orzecznictwa Trybunału Sprawiedliwości Unii Europejskiej (TSUE)[4].

Niniejszy dokument roboczy ma na celu aktualizację rozdziału pierwszego WP12 dotyczącego zasadniczej kwestii, jaką jest odpowiedni stopień ochrony danych osobowych w państwie trzecim, na terytorium lub w określonym sektorze lub określonych sektorach w tym państwie trzecim lub w organizacji międzynarodowej (zwanych dalej: „państwami trzecimi lub organizacjami międzynarodowymi"). Dokument ten będzie stale poddawany przeglądowi oraz, w razie potrzeby, aktualizowany w nadchodzących latach w oparciu o praktyczne doświadczenie zdobyte w trakcie stosowania RODO. Rozdział 2 („Stosowanie podejścia do państw, które ratyfikowały Konwencję o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych") i rozdział 3 („Stosowanie podejścia do samoregulacji przemysłu") dokumentu roboczego WP12 należy zaktualizować na późniejszym etapie.

Niniejszy dokument roboczy dotyczy wyłącznie decyzji stwierdzających odpowiedni stopień ochrony, które są aktami wykonawczymi[5] Komisji Europejskiej zgodnie z art. 45 RODO. Inne aspekty przekazywania danych osobowych do państw trzecich i organizacji międzynarodowych zostaną przeanalizowane w kolejnych dokumentach roboczych, które zostaną opublikowane oddzielnie (wiążące reguły korporacyjne, odstępstwa).

Celem niniejszego dokumentu jest dostarczenie wytycznych Komisji Europejskiej i Grupie Roboczej Art. 29 na podstawie RODO na potrzeby oceny stopnia ochrony danych osobowych w państwach trzecich i organizacjach międzynarodowych przez ustanowienie podstawowych zasad ochrony danych, które muszą być uwzględnione w ramach prawnych państwa trzeciego lub organizacji międzynarodowej w celu zapewnienia zasadniczej równoważności z ramami UE. Ponadto może on zapewnić wskazówki państwom trzecim i organizacjom międzynarodowym zainteresowanym uzyskaniem odpowiedniego stopnia ochrony. Zasady określone w niniejszym dokumencie roboczym nie są jednak skierowane bezpośrednio do administratorów danych ani podmiotów przetwarzających.

Niniejszy dokument składa się z czterech rozdziałów.

Rozdział 1: Ogólne informacje dotyczące pojęcia „odpowiedni stopień ochrony"

Rozdział 2: Aspekty proceduralne związane z ustaleniami dotyczącymi zapewnienia odpowiedniego stopnia ochrony na podstawie RODO

Rozdział 3: Ogólne zasady ochrony danych. Rozdział ten zawiera podstawowe ogólne zasady ochrony danych mające zapewnić, by stopień ochrony danych osobowych w państwie trzecim lub organizacji międzynarodowej był merytorycznie równoważny stopniowi określonemu w przepisach UE.

Rozdział 4: Niezbędne gwarancje dotyczące dostępu do danych w celu egzekwowania prawa i ze względów bezpieczeństwa narodowego mające na celu ograniczenie ingerencji w prawa podstawowe. W rozdziale tym określono niezbędne gwarancje dotyczące dostępu do danych w celu egzekwowania prawa i ze względów bezpieczeństwa narodowego zgodnie z wyrokiem TSUE w sprawie Schrems

[1] Utworzona zgodnie z art. 29 unijnej dyrektywy 95/46/WE o ochronie danych.

[2] WP12, „Dokument roboczy: Przekazywanie danych osobowych do państw trzecich: stosowanie art. 25 i 26 unijnej dyrektywy o ochronie danych" przyjęty przez Grupę Roboczą w dniu 24 lipca 1998 r.

[3] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Tekst mający znaczenie dla EOG).

[4] Uwzględniając wyrok Trybunału Sprawiedliwości z dnia 6 października 2015 r., Maximillian Schrems przeciwko Data Protection Commissioner, C-362/14.

[5] Więcej informacji na temat aktów wykonawczych można znaleźć w odpowiednich art. 45 ust. 3 i art. 93 ust. 2 RODO.



Nota informacyjna w sprawie wiążących reguł korporacyjnych (ang. *binding corporate rules*, BCR) dla przedsiębiorstw, dla których wiodącym organem nadzorczym jest Urząd Rzecznika Informacji (ang. *Information Commissioner's Office*, ICO)

Przyjęta 12 lutego 2019 r.

W sytuacji gdyby Zjednoczonego Królestwo wyszło z UE bez porozumienia, a ICO przestanie być jednym z organów nadzorczych właściwych w sprawach dotyczących wiążących reguł korporacyjnych (BCR), przedsiębiorstwa powinny wziąć pod uwagę poniższe:

• Grupy z siedzibą w Zjednoczonym Królestwie, które chcą złożyć wniosek o zatwierdzenie BCR: grupy takie powinny określić najbardziej odpowiedni wiodący organ nadzorczy w sprawie dotyczącej BCR w państwie członkowskim UE, zgodnie z kryteriami określonymi w pkt. 1.2 dokumentu WP 263.

• Obecnie rozpatrywanie wnioski: Grupy, dla których BCR są na etapie rozpatrywania przez ICO, muszą określić wiodący organ nadzorczy w sprawie dotyczącej BCR zgodnie z kryteriami określonymi w WP 263. Nowy wiodący organ nadzorczy w sprawie dotyczącej BCR przejmie wniosek i z chwilą wyjścia Zjednoczonego Królestwa z UE bez porozumienia formalnie rozpocznie nową procedurę.

Projekty BCR przedłożone EROD: jeśli w chwili wyjścia Zjednoczonego Królestwa z UE bez porozumienia projekt decyzji ICO zatwierdzającej BCR będzie w trakcie rozpatrywania przez EROD, grupa musi wyznaczyć nowy wiodący organ nadzorczy w sprawie dotyczącej BCR zgodnie z kryteriami określonymi w dokumencie WP 263. Nowy wiodący organ nadzorczy w sprawie dotyczącej BCR przejmie i ponownie przedłoży EROD projekt decyzji w celu zatwierdzenia EROD.

• Podmioty z zatwierdzonymi BCR: Podmioty z już zatwierdzonymi BCR powinny określić nowy wiodący organ nadzorczy w sprawie dotyczącej BCR zgodnie z kryteriami określonymi w dokumencie WP 263.

W każdym z powyższych scenariuszy organ nadzorczy będący potencjalnym nowym wiodącym organem nadzorczym w sprawie dotyczącej BCR rozważy w poszczególnych przypadkach i we współpracy z innymi zainteresowanymi organami nadzorczymi, czy jest właściwym wiodącym organem nadzorczym w sprawie dotyczącej BCR, i poinformuje grupę o swojej decyzji. W przypadku pytań lub próśb o dalsze informacje grupy są proszone o skontaktowanie się z ICO.

Rozdział 1: Ogólne informacje dotyczące pojęcia „odpowiedni stopień ochrony"

W art. 45 ust. 1 RODO ustanowiono zasadę, że przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej może nastąpić jedynie wówczas, gdy państwo trzecie, terytorium lub określony sektor lub określone sektory w tym państwie trzecim lub dana organizacja międzynarodowa zapewniają odpowiedni stopień ochrony.

Pojęcie „odpowiedni stopień ochrony", które istniało już na mocy dyrektywy 95/46, zostało doprecyzowane przez TSUE. W tym miejscu należy przypomnieć normę określoną przez TSUE w wyroku w sprawie Schrems, zgodnie z którą chociaż „stopień ochrony" w państwie trzecim musi być „merytorycznie równoważny" poziomowi gwarantowanemu w Unii, „środki, z jakich to państwo trzecie korzysta w tym względzie dla zapewnienia takiego stopnia ochrony, mogą różnić się od środków wprowadzonych w [Unii]"[6]. Dlatego też celem nie jest odzwierciedlenie punkt po punkcie prawodawstwa europejskiego, ale ustanowienie zasadniczych, tj. podstawowych, wymogów tego prawodawstwa.

Celem decyzji Komisji Europejskiej stwierdzających odpowiedni stopień ochrony jest formalne potwierdzenie ze skutkiem wiążącym dla państw członkowskich[7], że poziom ochrony danych osobowych w państwie trzecim lub organizacji międzynarodowej jest merytorycznie równoważny poziomowi ochrony danych osobowych w Unii Europejskiej[8]. Odpowiedni stopień ochrony można osiągnąć przez połączenie praw osób, których dane dotyczą, i obowiązków podmiotów, które przetwarzają dane lub sprawują kontrolę nad takim przetwarzaniem i nadzorem ze strony niezależnych organów. Przepisy o ochronie danych są jednak skuteczne tylko wtedy, gdy są możliwe do wyegzekwowania na drodze prawnej i przestrzegane w praktyce. Konieczne jest zatem rozważenie nie tylko treści przepisów mających zastosowanie do danych osobowych przekazywanych do państwa trzeciego lub organizacji międzynarodowej, ale także systemu stworzonego w celu zapewnienia skuteczności tych przepisów. Skuteczne mechanizmy egzekwowania prawa mają nadrzędne znaczenie dla skuteczności przepisów o ochronie danych.

W art. 45 ust. 2 RODO ustanowiono elementy, które Komisja Europejska uwzględnia podczas sprawdzania, czy stopień ochrony zapewniony w państwie trzecim lub organizacji międzynarodowej jest odpowiedni.

Na przykład Komisja uwzględnia praworządność, poszanowanie praw człowieka i podstawowych wolności, odpowiednie ustawodawstwo, istnienie i skuteczne działanie co najmniej jednego niezależnego organu nadzorczego oraz międzynarodowe zobowiązania zaciągnięte przez dane państwo trzecie lub daną organizację międzynarodową.

Jasne jest zatem, że jakakolwiek konstruktywna analiza odpowiedniej ochrony musi obejmować dwa podstawowe elementy: treść mających zastosowanie przepisów oraz środki służące zapewnieniu ich skutecznego stosowania. Do Komisji Europejskiej należy regularne sprawdzanie, czy obowiązujące przepisy są skuteczne w praktyce.

„Podstawowe" zasady ochrony „treści" danych i wymogi „proceduralne / dotyczące egzekwowania", które mogłyby być postrzegane jako minimalny wymóg zapewnienia odpowiedniej ochrony, wynikają z Karty praw podstawowych Unii Europejskiej i RODO. Ponadto należy również uwzględnić inne umowy międzynarodowe dotyczące ochrony danych osobowych, np. Konwencję o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych[9].

[6] Wyrok Trybunału Sprawiedliwości z dnia 6 października 2015 r., Maximillian Schrems przeciwko Data Protection Commissioner, C-362/14, pkt 73, 74.
[7] Art. 288 ust. 2 TFUE.
[8] Wyrok Trybunału Sprawiedliwości z dnia 6 października 2015 r., Maximillian Schrems przeciwko Data Protection Commissioner, C-362/14, pkt 52.
9 Motyw 105 RODO.

Należy również zwrócić uwagę na ramy prawne dotyczące dostępu organów publicznych do danych osobowych. Dalsze wskazówki na ten temat znajdują się w dokumencie roboczym nr 237 (tj. w dokumencie w sprawie niezbędnych gwarancji)[10] dotyczącym gwarancji w kontekście nadzoru.

Przepisy ogólne dotyczące ochrony danych osobowych i prywatności w państwie trzecim nie są wystarczające. Wręcz przeciwnie, w ramach prawnych państwa trzeciego lub organizacji międzynarodowej należy zawrzeć przepisy szczególne regulujące konkretne potrzeby związane z praktycznie istotnymi aspektami prawa do ochrony danych osobowych. Przepisy te muszą być możliwe do wyegzekwowania na drodze prawnej.

Rozdział 2: Aspekty proceduralne związane z ustaleniami dotyczącymi zapewnienia odpowiedniego stopnia ochrony na podstawie RODO

Aby Europejska Rada Ochrony Danych mogła wypełnić swoje zadanie polegające na doradzaniu Komisji Europejskiej zgodnie z art. 70 ust. 1 lit. s) RODO, powinna ona otrzymać odpowiednią dokumentację, w tym odpowiednią korespondencję i ustalenia dokonane przez Komisję Europejską. W przypadku gdy ramy prawne są złożone, dokumentacja taka powinna obejmować wszelkie sprawozdania przygotowane na temat stopnia ochrony danych osobowych w państwie trzecim lub organizacji międzynarodowej. W każdym razie informacje dostarczone przez Komisję Europejską powinny być wyczerpujące i powinny umożliwić Europejskiej Radzie Ochrony Danych dokonanie własnej oceny stopnia ochrony danych osobowych w państwie trzecim. Europejska Rada Ochrony Danych przedstawi w odpowiednim czasie opinię na temat ustaleń Komisji Europejskiej oraz wskaże ewentualne braki w ramach dotyczących odpowiedniego stopnia ochrony. Europejska Rada Ochrony Danych postara się również zaproponować zmiany lub poprawki, aby zaradzić ewentualnym brakom.

Zgodnie z art. 45 ust. 4 RODO do Komisji Europejskiej należy monitorowanie na bieżąco zmian mogących wpłynąć na obowiązywanie decyzji stwierdzającej odpowiedni stopień ochrony.

Art. 45 ust. 3 RODO stanowi, że okresowy przegląd musi odbywać się przynajmniej raz na cztery lata. Są to jednak ogólne ramy czasowe, które muszą zostać dostosowane do każdego państwa trzeciego lub organizacji międzynarodowej zgodnie z decyzją stwierdzającą odpowiedni stopień ochrony. W zależności od konkretnych okoliczności uzasadniony może być krótszy cykl przeglądu. Ponadto incydenty lub inne informacje na temat ram prawnych lub zmiany tych ram prawnych w danym państwie trzecim lub organizacji międzynarodowej mogą spowodować konieczność dokonania przeglądu przed planowanym terminem. Wydaje się również właściwe, aby pierwszy przegląd całkowicie nowej decyzji stwierdzającej odpowiedni stopień ochrony przeprowadzono dosyć szybko i stopniowo dostosowywano cykl przeglądu w zależności od wyniku.

Biorąc pod uwagę upoważnienie do przekazywania Komisji Europejskiej opinii na temat tego, czy państwo trzecie, terytorium lub określony sektor lub określone sektory w tym państwie trzecim lub organizacja międzynarodowa nie zapewniają już odpowiedniego stopnia ochrony, Europejska Rada Ochrony Danych musi, w odpowiednim czasie, otrzymać istotne informacje dotyczące monitorowania przez Komisję Europejską istotnych zmian w tym państwie trzecim lub organizacji międzynarodowej. W związku z tym Europejska Rada Ochrony Danych powinna być na bieżąco informowana o każdym procesie przeglądu i misji przeglądowej w państwie trzecim lub organizacji międzynarodowej. Europejska Rada Ochrony Danych z zadowoleniem przyjęłaby zaproszenie do udziału w takich procesach i misjach przeglądowych.

Należy również zauważyć, że zgodnie z art. 45 ust. 5 RODO Komisja Europejska ma prawo uchylić, zmienić lub zawiesić istniejące decyzje stwierdzające odpowiedni stopień ochrony. W procedurze uchylania, zmieniania lub zawieszania powinna zatem uczestniczyć Europejska Rada Ochrony Danych, od której wymaga się przedstawienia opinii zgodnie z art. 70 ust. 1 lit. s).

Ponadto, jak obecnie uznano w art. 58 ust. 5 RODO i zgodnie z wyrokiem TSUE w sprawie Schrems, organy ochrony danych muszą mieć możliwość wszczęcia postępowania prawnego, jeżeli uznają, że zarzuty danej osoby dotyczące decyzji stwierdzającej odpowiedni stopień ochrony są zasadne: „W tym względzie do krajowego ustawodawcy należy ustanowienie drogi prawnej umożliwiającej krajowemu organowi nadzorczemu podniesienie zarzutów, które uważa on za zasadne, przed sądami krajowymi, po to, aby te ostatnie, jeśli podzielają wątpliwości tego organu co do ważności decyzji Komisji, wystąpiły z wnioskiem o wydanie orzeczenia w trybie prejudycjalnym w celu zbadania ważności tej decyzji"[11].

[10] Dokument Roboczy 01/2016 w sprawie uzasadnienia ingerencji w podstawowe prawa do prywatności i ochrony danych poprzez środki nadzoru w przypadku przekazywania danych osobowych (niezbędne gwarancje europejskie), 16/EN WP 237, 13 kwietnia 2016 r.

[11] Wyrok Trybunału Sprawiedliwości z dnia 6 października 2015 r., Maximillian Schrems przeciwko Data Protection Commissioner, C-362/14, pkt 65.

Rozdział 3: Ogólne zasady ochrony danych mające zapewnić, by stopień ochrony danych osobowych w państwie trzecim, na terytorium lub w określonym sektorze lub określonych sektorach w tym państwie trzecim lub organizacji międzynarodowej był merytorycznie równoważny stopniowi określonemu w przepisach UE

System państwa trzeciego lub organizacji międzynarodowej musi zawierać następujące podstawowe zasady i mechanizmy ochrony treści oraz zasady i mechanizmy proceduralne / dotyczące wdrażania w odniesieniu do danych osobowych:

A. <u>Zasady dotyczące treści:</u>

1) Pojęcia

Powinny istnieć podstawowe pojęcia lub zasady dotyczące ochrony danych osobowych. Nie muszą one odzwierciedlać terminologii RODO, ale powinny odzwierciedlać pojęcia zawarte w europejskim prawie w dziedzinie ochrony danych i być z nimi spójne. Przykładowo RODO zawiera następujące istotne pojęcia: „dane osobowe", „przetwarzanie danych osobowych", „administrator danych", „podmiot przetwarzający", „odbiorca" i „dane wrażliwe".

2) Podstawy zgodnego z prawem i rzetelnego przetwarzania danych do prawnie uzasadnionych celów

Dane muszą być przetwarzane w sposób zgodny z prawem, rzetelny i prawnie uzasadniony.

Należy odpowiednio jasno określić uzasadnione podstawy, w ramach których można zgodnie z prawem, rzetelnie i w sposób prawnie uzasadniony przetwarzać dane osobowe. W przepisach unijnych przewidziano kilka takich uzasadnionych prawnie podstaw, w tym np. przepisy prawa krajowego, zgodę osoby, której dane dotyczą, wykonanie umowy lub prawnie uzasadniony interes realizowany przez administratora lub przez stronę trzecią, który nie jest nadrzędny wobec interesów osoby fizycznej.

3) Zasada ograniczenia celu

Dane powinny być przetwarzane w określonym celu, a następnie wykorzystywane tylko w takim zakresie, w jakim nie jest to niezgodne z celem przetwarzania danych.

4) Zasada jakości danych oraz proporcjonalności

Dane powinny być prawidłowe i w razie potrzeby uaktualniane. Dane powinny być adekwatne, stosowne i niewykraczające poza cele, w których są przetwarzane.

5) Zasada zatrzymywania danych

Co do zasady dane nie powinny być przechowywane przez okres dłuższy, niż jest to niezbędne do celów, w których te dane osobowe są przetwarzane.

6) Zasada bezpieczeństwa i poufności

Każdy podmiot przetwarzający dane osobowe powinien zagwarantować przetwarzanie danych osobowych w sposób zapewniający bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych. Poziom bezpieczeństwa powinien uwzględniać stan wiedzy technicznej oraz związane z nim koszty.

7) Zasada przejrzystości

Każda osoba fizyczna powinna być informowana o wszystkich głównych elementach przetwarzania jej danych osobowych w jasnej, łatwo dostępnej, zwięzłej, przejrzystej i zrozumiałej formie. Informacje takie powinny obejmować cel przetwarzania danych, tożsamość administratora danych, przyznane mu prawa oraz inne informacje w zakresie, w jakim jest to niezbędne do zapewnienia rzetelności. W pewnych okolicznościach możliwe są wyjątki od tego prawa do informacji, np. w celu ochrony postępowania przygotowawczego, ze względu na bezpieczeństwo narodowe, niezależność sądów i dobro postępowania sądowego lub z uwagi na inne ważne cele leżące w ogólnym interesie publicznym, jak w przypadku art. 23 RODO.

8) Prawo dostępu, prawo do sprostowania i usunięcia danych oraz prawo do sprzeciwu

Osoba, której dane dotyczą, powinna mieć prawo do uzyskania potwierdzenia, czy jej dane osobowe są przetwarzane, oraz prawo dostępu do swoich danych, w tym do otrzymania kopii wszystkich danych jej dotyczących, które są przetwarzane.

Osoba, której dane dotyczą, powinna mieć prawo do uzyskania, w stosownych przypadkach, sprostowania swoich danych osobowych, z określonych powodów, np. w przypadku wykazania, że są one nieprawidłowe lub niekompletne, oraz prawo do usunięcia swoich danych osobowych, np. gdy ich przetwarzanie nie jest już konieczne lub jest niezgodne z prawem.

Osoba, której dane dotyczą, powinna mieć również prawo do wniesienia w dowolnym momencie, z ważnych i prawnie uzasadnionych przyczyn związanych z jej szczególną sytuacją, sprzeciwu wobec przetwarzania jej danych osobowych na szczególnych warunkach określonych w przepisach prawnych państwa trzeciego. W RODO warunki te obejmują np. przypadki, gdy przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub gdy jest niezbędne do sprawowania władzy publicznej powierzonej administratorowi lub gdy przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią.

Wykonanie tych praw nie powinno być nadmiernie uciążliwe dla osoby, której dane dotyczą. Możliwe ograniczenia tych praw mogą istnieć np. w celu ochrony postępowania przygotowawczego, ze względu na bezpieczeństwo narodowe, niezależność sądów i dobro postępowania sądowego lub z uwagi na inne ważne cele leżące w ogólnym interesie publicznym, jak w przypadku art. 23 RODO.

9) Ograniczenia dotyczące dalszego przekazywania danych

Dalsze przekazywanie danych osobowych przez pierwotnego odbiorcę pierwotnego przekazywania danych powinno być dozwolone tylko wtedy, gdy dalszy odbiorca (tj. odbiorca dalszego przekazywania) również podlega przepisom (w tym przepisom umownym) zapewniającym odpowiedni stopień ochrony i przestrzega odpowiednich instrukcji podczas przetwarzania danych w imieniu administratora danych. Dalsze przekazywanie danych nie może podważać stopnia ochrony osób fizycznych, których dane są przekazywane. Pierwotny odbiorca danych przekazywanych z UE jest odpowiedzialny za zapewnienie odpowiednich zabezpieczeń w odniesieniu do dalszego przekazywania danych w przypadku braku decyzji stwierdzającej odpowiedni stopień ochrony. Takie dalsze przekazywanie danych powinno być prowadzone jedynie w ograniczonych i określonych celach oraz dopóki istnieje podstawa prawna takiego przetwarzania.

B. <u>Przykłady dodatkowych zasad dotyczących treści, które mają być stosowane do konkretnych rodzajów przetwarzania:</u>

1) Szczególne kategorie danych osobowych

Jeżeli przetwarzanie obejmuje „szczególne kategorie danych osobowych", powinny istnieć szczególne zabezpieczenia[12]. Kategorie te powinny odzwierciedlać kategorie określone w art. 9 i 10 RODO. Ochronę taką należy zapewnić przez wprowadzenie bardziej rygorystycznych wymogów dotyczących przetwarzania danych osobowych, takich jak np. udzielenie przez osobę, której dane dotyczą, wyraźnej zgody na przetwarzanie danych, lub poprzez dodatkowe środki bezpieczeństwa.

2) Marketing bezpośredni

W przypadku gdy dane są przetwarzane do celów marketingu bezpośredniego, osoba, której dane dotyczą, powinna mieć możliwość wniesienia w dowolnym momencie i bez ponoszenia żadnych kosztów sprzeciwu wobec przetwarzania jej danych osobowych do takich celów.

3) Zautomatyzowane podejmowanie decyzji i profilowanie

Decyzje oparte wyłącznie na zautomatyzowanym przetwarzaniu (zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach), w tym profilowaniu, które wywołują skutki prawne lub istotnie wpływają na osobę, której dane dotyczą, mogą być podejmowane jedynie pod pewnymi warunkami określonymi w ramach prawnych państwa trzeciego. W ramach europejskich warunki takie obejmują m.in. potrzebę uzyskania wyraźnej zgody osoby, której dane dotyczą, lub konieczność uzyskania takiej decyzji do celów zawarcia umowy. Jeżeli decyzja nie jest zgodna z takimi warunkami określonymi w ramach prawnych państwa trzeciego, osoba, której dane dotyczą, powinna mieć prawo do niepodlegania takiej decyzji. Przepisy państwa trzeciego powinny w każdym przypadku przewidywać niezbędne zabezpieczenia, w tym prawo do uzyskania informacji o konkretnych powodach podjęcia danej decyzji oraz o jej logice, prawo do skorygowania nieprawidłowych lub niekompletnych informacji oraz prawo do zakwestionowania decyzji, jeżeli została ona podjęta na podstawie błędnego stanu faktycznego.

C. <u>Mechanizmy proceduralne i mechanizmy egzekwowania prawa:</u>

Mimo że środki, z których korzysta państwo trzecie w celu zapewnienia odpowiedniego stopnia ochrony mogą się różnić od środków stosowanych w Unii Europejskiej[13], system zgodny z systemem europejskim musi charakteryzować się istnieniem następujących elementów.

1) Właściwy niezależny organ nadzorczy

Powinien istnieć co najmniej jeden niezależny organ nadzorczy odpowiedzialny za monitorowanie, zapewnianie i egzekwowanie zgodności z przepisami dotyczącymi ochrony danych osobowych i prywatności w państwie trzecim. Organ nadzorczy powinien działać w sposób w pełni niezależny i bezstronny podczas wypełniania swoich zadań i wykonywania swoich uprawnień oraz w toku tych działań nie powinien zwracać się o żadne instrukcje ani ich przyjmować. W tym kontekście organ nadzorczy powinien dysponować wszystkimi niezbędnymi i dostępnymi uprawnieniami i funkcjami w celu zapewnienia przestrzegania praw do ochrony danych osobowych i propagowania wiedzy na ten temat. Należy również zastanowić się nad personelem i budżetem organu nadzorczego. Organ nadzorczy powinien być również w stanie prowadzić dochodzenia z urzędu.

2) System ochrony danych musi zapewnić odpowiedni stopień zgodności

System państwa trzeciego powinien zapewniać wysoki stopień rozliczalności i świadomości wśród administratorów danych oraz podmiotów przetwarzających dane osobowe w ich imieniu w zakresie ich obowiązków, zadań i zakresu odpowiedzialności oraz wśród osób, których dane dotyczą, w zakresie ich praw i sposobów ich wykonywania. Istnienie skutecznych i zniechęcających sankcji może odegrać ważną rolę w zapewnieniu poszanowania przepisów, podobnie jak sprawić to mogą systemy bezpośredniej weryfikacji przez organy, audytorów lub niezależnych inspektorów ochrony danych.

3) Rozliczalność

Ramy ochrony danych osobowych obowiązujące w państwie trzecim powinny zobowiązywać administratorów danych lub podmioty przetwarzające dane osobowe w ich imieniu do przestrzegania tych ram oraz nakładać na nich obowiązek, by byli w stanie wykazać zgodność z ramami, w szczególności właściwemu organowi nadzorczemu. Tego rodzaju środki mogą obejmować m.in. ocenę skutków w zakresie ochrony danych, prowadzenie rejestrów lub dzienników czynności przetwarzania danych przez odpowiedni okres, wyznaczenie urzędnika ds. ochrony danych lub uwzględnienie ochrony danych w fazie projektowania lub domyślnej ochrony danych.

4) System ochrony danych musi zapewniać wsparcie i pomoc poszczególnym osobom, których dane dotyczą, w wykonywaniu przysługujących im praw i korzystaniu z odpowiednich mechanizmów dochodzenia roszczeń

Osoba fizyczna powinna mieć możliwość skorzystania ze środków ochrony prawnej w celu szybkiego i skutecznego egzekwowania swoich praw, bez nadmiernych kosztów oraz w celu zapewnienia przestrzegania tych praw. W tym celu muszą istnieć mechanizmy nadzoru pozwalające na niezależne rozpatrywanie skarg oraz umożliwiające identyfikowanie w praktyce wszelkich naruszeń prawa do ochrony danych osobowych i poszanowania życia prywatnego oraz nakładanie kar za takie naruszenia.

W przypadku nieprzestrzegania przepisów osobie, której dane dotyczą, należy zapewnić skuteczne administracyjne i sądowe środki zaskarżenia, w tym odszkodowanie z tytułu szkód poniesionych w wyniku niezgodnego z prawem przetwarzania jej danych osobowych. Jest to najważniejszy element, który wiąże się z systemem niezależnego orzekania lub arbitrażu, umożliwiający wypłatę odszkodowania i, w stosownych przypadkach, nałożenie sankcji.

[12] Takie szczególne kategorie zostały również określone jako „dane wrażliwe" w motywie 10 RODO.
[13] Wyrok Trybunału Sprawiedliwości z dnia 6 października 2015 r., Maximillian Schrems przeciwko Data Protection Commissioner, C-362/14, pkt 74.

Rozdział 4: Niezbędne gwarancje w państwach trzecich dotyczące dostępu do danych w celu egzekwowania prawa i ze względów bezpieczeństwa narodowego mające na celu ograniczenie ingerencji w prawa podstawowe

Oceniając, czy stopień ochrony jest odpowiedni, na mocy art. 45 ust. 2 lit. a) Komisja jest zobowiązana uwzględnić „odpowiednie ustawodawstwo – zarówno ogólne, jak i sektorowe – w tym w dziedzinie bezpieczeństwa publicznego, obrony, bezpieczeństwa narodowego i prawa karnego oraz dostępu organów publicznych do danych osobowych, a także wdrażanie takiego ustawodawstwa (…)".

W wyroku w sprawie Schrems TSUE zauważył, że „wyrażenie »odpowiedni stopień ochrony« należy rozumieć jako wymagające od tego państwa trzeciego skutecznego zapewnienia, ze względu na jego ustawodawstwo wewnętrzne lub zobowiązania międzynarodowe, poziomu ochrony podstawowych praw i wolności merytorycznie równoważnego poziomowi gwarantowanemu w Unii na mocy dyrektywy 95/46 w związku z kartą". Jakkolwiek środki, z jakich to państwo trzecie korzysta w tym względzie, mogą różnić się od środków wprowadzonych w Unii, środki te muszą być jednak w praktyce skuteczne[14].

W tym kontekście Trybunał zauważył również krytycznie, że poprzednia decyzja w sprawie „bezpiecznej przystani" „nie zawiera żadnego stwierdzenia dotyczącego istnienia w Stanach Zjednoczonych reguł o charakterze ogólnopaństwowym służących do ograniczenia ewentualnych ingerencji w prawa podstawowe osób, których dane zostały przekazane z Unii do Stanów Zjednoczonych, ingerencji, które organy państwowe tego kraju mogłyby dokonywać przy okazji dążenia do realizacji uzasadnionego prawem celu, takiego jak bezpieczeństwo narodowe".

Grupa Robocza Art. 29 określiła w dokumencie roboczym WP237 przyjętym w dniu 13 kwietnia 2016 r. niezbędne gwarancje odzwierciedlające orzecznictwo TSUE i orzecznictwo związane z Konwencją o ochronie praw człowieka i podstawowych wolności w obszarze nadzoru. Chociaż zalecenia sformułowane w WP237 pozostają w mocy i powinny być brane pod uwagę przy ocenie, czy państwo trzecie zapewnia odpowiedni stopień ochrony w obszarze nadzoru, stosowanie tych gwarancji może się różnić w obszarach dostępu do danych w celu egzekwowania prawa i ze względów bezpieczeństwa narodowego. Aby poniższe cztery gwarancje zostały uznane za odpowiednie, muszą być jednak przestrzegane przez wszystkie państwa trzecie w odniesieniu do dostępu do danych, zarówno ze względów bezpieczeństwa narodowego, jak i do celów egzekwowania prawa:

1) **Przetwarzanie powinno opierać się na jasnych, precyzyjnych i dostępnych przepisach (podstawa prawna).**

2) **Należy wykazać konieczność i proporcjonalność w odniesieniu do zamierzonych prawnie uzasadnionych celów.**

3) **Przetwarzanie danych musi podlegać niezależnemu nadzorowi.**

4) **Osoby fizyczne muszą mieć dostęp do skutecznych środków ochrony prawnej.**

[14] Wyrok Trybunału Sprawiedliwości z dnia 6 października 2015 r., Maximillian Schrems przeciwko Data Protection Commissioner, C-362/14, pkt 74.