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 I

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 978-83-63484-61-3

SPIS TREŚCI

SPIS TABEL

SPIS RYSUNKÓW

WPROWADZENIE

Dnia 14 kwietnia 2016 roku Parlament Europejski przyjął ostateczną treść nowego prawa ochrony danych osobowych, mającego zastąpić niemal cały dotychczasowy reżim prawny obowiązujący w tym zakresie w przestrzeni Unii Europejskiej. 4 maja 2016 roku w Dzienniku Urzędowym Unii Europejskiej zostały opublikowane oficjalne teksty aktów prawnych składających się na reformę ochrony danych osobowych. Zgodnie z art. 99, jako normą temporalną, rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku 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), weszło w życie 20. dnia po publikacji w Dzienniku Urzędowym Unii Europejskiej, natomiast – co istotne – jest stosowane od dnia 25 maja 2018 roku.

Polski porządek prawny uzupełnia ustawa z 10 maja 2018 roku o ochronie danych osobowych, ustawa z dnia 9 maja 2018 roku o przetwarzaniu danych dotyczących przelotu pasażera, oraz ustawa z dnia 14 grudnia 2018 roku o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, które to akty prawne dokonały implementacji szeregu dyrektyw sektorowych, w tym przykładowo dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 roku 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). Przyjęcie przepisów wykonawczych oraz sektorowych dopełniło strukturę reformy prawodawstwa ODO (GDPR) w Polsce.

Do czasu wejścia w życie nowych przepisów obowiązywała 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, oraz relewantne krajowe przepisy implementacyjne, w tym przede wszystkim ustawa z dnia 29 sierpnia 1997 roku o ochronie danych osobowych wraz z przepisami wykonawczymi do niej.

Przy tym należy zaznaczyć, że ową strukturę – chociażby z uwagi na złożony przedmiot regulacji – należy charakteryzować w modelu procesowym, albowiem jest ona dynamiczna

i „żywa", będąc poddawana nowelizacjom i wynikającym z nich modyfikacjom. Stąd na model prawny i społeczny ochrony danych osobowych oraz szerzej prywatności, należy patrzeć z perspektywy, uwzględniającej pierwotne dokumenty międzynarodowe kreujące ten system w pierwszej fazie, kolejne akty prawne powstające na łonie UE, stanowiące swoistą drugą falę, oraz wreszcie najnowszą i najdonioślejszą reformę płynącą z rozporządzenia 2016/679 oraz aktów powiązanych. Analiza krytyczna całości historycznej pozwala dokonać porównań, a nawet podsumowań, zarówno z pozycji wybranych zmian i nowelizacji, jak i uwag ogólnych, generalnie odnoszących się do oceny konkretnego modelu. System GDPR po pierwsze nie narodził się 25 maja 2018 roku, po drugie nie wszystkie przecież reformy (na tle poprzednich rozwiązań) musiały być trafione i skuteczne, po trzecie wreszcie każda zmiana ma swoje konsekwencje społeczne czy ekonomiczne (np. koszty po stronie podmiotów adresatów norm zobowiązanych do wdrożenia dodatkowych wymogów).

Od pewnego czasu można zaobserwować przesilenie w sferze relacji informacyjnych opartych o wymianę danych przy pomocy narzędzi teleinformatycznych. Po pierwsze zarysowuje się trend podnoszenia poziomu świadomości społecznej w zakresie wszelkich konsekwencji wynikających z takiej formy komunikacji, w szczególności zagrożeń prywatności. Po drugie coraz wyraźniejsza jest presja opinii publicznej, która dostrzega potrzebę zapewnienia realnego nadzoru nad procesami gromadzenia i przetwarzania danych w ramach ponadkrajowych modeli wymiany gospodarczej i politycznej. Pomimo oczywistych trudności wynikających z samego charakteru transferów informacyjnych, których bezpieczeństwo jest podatne na łatwe przełamania w postaci infekcji, kradzieży, podszywania się czy podsłuchów (szczególnie w ramach ogólnodostępnej sieci), należy uznać, że nie może stanowić to wytłumaczenia, ani usprawiedliwienia dla braku efektywnego systemu ochrony danych osobowych. Stąd co jakiś czas pojawiają się kolejne próby bądź uszczelnienia, czy też poprawienia istniejącego modelu, bądź stworzenia nowego – doskonalszego.

Należy wyeksponować, że kolejne wersje systemu nie stanowiły jedynie wyzwania legislacyjnego czy badawczego, ale przede wszystkim miały swoje konsekwencje praktyczne, chociażby bezpośrednio rzutując na sposób opracowywania i wdrażania dokumentacji ochrony danych osobowych. Każda zmiana implikowała obowiązki po stronie administratorów danych. Następujące po sobie reformy *de facto* nakładały na administratorów obowiązek dokonania przeglądu istniejących procedur ochrony danych osobowych pod kątem dostosowania do nowych wymogów prawnych wraz z koniecznością wdrożenia zmian dostosowawczych. Po pierwsze na poziomie identyfikacji zmian i obowiązków zgodności (*compliance*), po drugie na poziomie implementacyjnym. W tym względzie wymagało to od administratorów co najmniej: (a) sprawdzenia świadomości oraz gotowości do wdrożenia nowych procedur bezpieczeństwa, (b) przeprowadzenia audytu zgodności systemu bezpieczeństwa danych osobowych w jednostce organizacyjnej z aktualnymi przepisami, (c) opracowania procedur pozwalających na stwierdzenie zgodności systemu z aktualnie obowiązującymi przepisami, (e) opracowania raportu

w zakresie przygotowania i gotowości jednostki organizacyjnej do wdrożenia i przyjęcia nowych procedur, wreszcie (f) wdrożenia w jednostce organizacyjnej wszystkich procedur pozwalających na stwierdzenie zgodności z systemu z nowymi przepisami.

Poddając analizie prawnej wybrane, relewantne regulacje, pod kątem niezbędności aktualizacji dossier ochrony danych osobowych, oraz faktycznego wdrażania procedur bezpieczeństwa, i w tym w celu minimalizacji ryzyka pozostawania w stanie nieprzestrzegania norm oraz eliminacji potencjalnej odpowiedzialności (karnej, cywilnej oraz administracyjnej administratora danych), potrzebne wydawało się dokonanie porównania zmieniającego się otoczenia prawnego. Mimo wielu zmian przepisów nie zmieniła się bowiem pozycja administratora jako podmiotu decydującego o celach i środkach przetwarzania danych osobowych. Każdy administrator danych jest cały czas zobowiązany, mając świadomość zagrożeń, podejmować wszelkie możliwe działania niezbędne dla zapewnienia bezpieczeństwa danych osobowych, rozumianego jako utrzymanie poufności, integralności, dostępności, rozliczalności, autentyczności, oraz niezaprzeczalności.

Kilka lat funkcjonowania nowego systemu GDPR (ODO) należy uznać za dobry moment na dokonanie oceny i podsumowań (w oparciu o dostępne źródła) dotychczasowego dorobku normatywnego oraz praktyki stosowania konkretnego instrumentarium prawnego. W szczególności, iż należy się spodziewać, że aktualny model nie jest docelowym i ostatnim systemem ochrony danych osobowych. Zaprezentowane i przeanalizowane wybrane zmiany pozwalają prześledzić kierunek zmian, cele które legislator chciał osiągnąć, wreszcie generalną tendencję, którą podąża system ochrony danych osobowych.

Praca (obok wprowadzenia, podsumowań rozdziałów i wniosków końcowych) składa się z trzech bloków tematycznych i w konsekwencji materialnoprawych: (1) analizy wybranych reform systemu ODO obowiązującego w Polsce w latach 1997–2018, (2) przeglądu wybranych instytucji prawnych wprowadzonych rozporządzeniem 2016/679 (RODO) oraz przepisami powiązanymi, (3) deskrypcją systemu kar za delikty na systemie ODO, w tym odpowiedzialności administracyjnej, cywilnej, odszkodowawczej, dyscyplinarnej, pracowniczej oraz karnej. Całość wpisana jest w: (a) przegląd przyczyn społecznych, gospodarczych, technologicznych, politycznych (cywilizacyjnych), które stanęły u podstaw dokonywanych konsekwentnie zmian systemu ODO oraz wprowadzenia dużej reformy GDPR w 2018 roku, (b) analizę ewolucji treści (kolejnych wersji) nowej ustawy o ochronie danych osobowych wraz z przepisami sektorowymi, (c) zestawienie przepisów szczegółowych.

Uzupełnieniem pracy są wybrane załączniki, newralgiczne dla prawidłowości stosowania ochrony danych osobowych, w tym m.in.: komunikat PUODO czy opinia EROD w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania, decyzje wykonawcze Komisji w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich, odpowiednie wzory zawiadomień o wyznaczeniu nowego lub odwołaniu dotychczasowego Inspektora Ochrony

Danych, zgłoszenia naruszenia ochrony danych osobowych, czy wzory umów powierzenia przetwarzania oraz udostępnienia danych osobowych. Zwieńczeniem natomiast jest zestawienie wybranych, ważkich dla praktyków wzorów dokumentacji systemu ochrony danych osobowych, w szczególności Polityki Ochrony Danych Osobowych i Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych wraz ze stosowanym komentarzem oraz uzasadnieniem zmian zakresu dokumentacyjnego.

Przedmiot niniejszej pracy, choć wieloaspektowy, łączy dziedziny nauk prawnych, ekonomicznych, o polityce czy o zarządzaniu. Wykorzystano możliwości analizy systemowej, w dziedzinie rekonstrukcji i analizy relacji między poszczególnymi elementami kluczowymi dla pracy. Metoda porównawcza oraz relacyjna pozwoliła ukazać zjawiska w ujęciu procesowym. Praca zawiera uwagi uniwersalne zarówno samego autora, oraz cytowanych komentatorów, jak również formułuje wnioski *de lege ferenda*. Zestawia także refleksje jakie płyną z danych statystycznych. Z uwagi na fakt, że przedmiotem analizy jest przestrzeń systemu ochrony danych osobowych, w szczególności wynikająca z rozporządzenia 2016/679, *ergo* zagadnienia charakteryzujące się obszernością mogą nie uwzględniać niektórych szczegółowych regulacji, orzeczeń czy poglądów, co należy uwzględnić w ramach bardziej pogłębionej analizy przedmiotu.

OTOCZENIE PRAWNE

Kwestie przetwarzania oraz ochrony danych osobowych były przedmiotem powstających od lat siedemdziesiątych w Europie aktów prawnych. Regulacje rodziły się na wielu płaszczyznach normatywnych: po pierwsze w prawie międzynarodowym, w konsekwencji później europejskim (wspólnotowym, unijnym), w prawie krajowym na wszelkich jego szczeblach (na poziomie konstytucyjnym, ustawowym i wykonawczym) jako prawo generalne, oraz sektorowe (*lex specialis*). Przy tym należy zaznaczyć, że najpierw powstawały lokalne ustawy o ochronie danych osobowych (np. w landach federacyjnych w Niemczech, we Francji, czy w Szwecji), by następnie, w obliczu pogłębiającej się integracji europejskiej, oraz uciążliwości wynikającej z odmienności przepisów w różnych państwach członkowskich, przyjmować dokumenty (rekomendacje, konwencje) na forum Rady Europy (w szczególności Konwencja nr 108), Unii Europejskiej (w szczególności Dyrektywa 95/46/WE), początkowo o charakterze generalnym, następnie sektorowym. Poniżej zestawienie wybranych aktów międzynarodowych, europejskich oraz krajowych (ujęcie historyczne).

1) Normy europejskie międzynarodowo-prawne, w tym wybrane sektorowe: (1) Konwencja Nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych sporządzona w Strasburgu dnia 28 stycznia 1981 r., (2) Rezolucja (73) 22 z 26.09.1973 r. dotycząca ochrony prywatności jednostek w odniesieniu do elektronicznych banków danych w sektorze prywatnym, Komitet Ministrów Rady Europy, (3) Rezolucja (74) 29 z 20.09.1974 r. dotycząca ochrony prywatności jednostek w odniesieniu do elektronicznych banków danych w sektorze publicznym, Komitet Ministrów Rady Europy, (4) Rekomendacja (1986) 1 z 23 stycznia 1986 r. w sprawie ochrony prywatności w Internecie – wytyczne w sprawie ochrony danych osobowych używanych dla celów zabezpieczeń społecznych, Komitet Ministrów Rady Europy, (5) Rekomendacja R (1999) 5 23 lutego 1999 r. w sprawie ochrony prywatności w Internecie – wytyczne w sprawie ochrony osób w zakresie gromadzenia i przetwarzania danych osobowych na „infostradach", Komitet Ministrów Rady Europy, (6) Rekomendacja (2010) 13 z 23.11.2010 r. w sprawie ochrony osób w związku z automatycznym przetwarzaniem danych osobowych podczas tworzenia profili, Komitet Ministrów Rady Europy;

2) Normy unijne generalne: (1) art. 16 Traktatu o funkcjonowaniu UE (po zmianach wynikających z Traktatu z Lizbony)[1]; (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)[2], (3) 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[3], (4) 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];
3) Normy unijne generalne do wejścia w życie rozporządzenia 2016/679: (1) rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych[5], (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 oraz swobodnego przepływu tych danych[6];
4) Normy unijne sektorowe (wybrane): (1) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/794 z dnia 11 maja 2016 r. w sprawie Agencji Unii Europejskiej ds. Współpracy Organów Ścigania (Europol), zastępujące i uchylające decyzje Rady 2009/371/WSiSW, 2009/934/WSiSW, 2009/935/WSiSW, 2009/936/WSiSW i 2009/968/WSiSW[7], (2) dyrektywa 2004/82/WE z dnia 29 kwietnia 2004 r. w sprawie zobowiązania przewoźników do przekazywania danych pasażerów (dyrektywa API)[8], (3) dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/681 z dnia 27 kwietnia 2016 r. w sprawie wykorzystywania danych dotyczących przelotu pasażera (danych PNR) w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości,

[1] (1) Każda osoba ma prawo do ochrony danych osobowych jej dotyczących; (2) Parlament Europejski i Rada, stanowiąc zgodnie ze zwykłą procedurą ustawodawczą, określają zasady dotyczące ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez instytucje, organy i jednostki organizacyjne Unii oraz przez państwa członkowskie w wykonywaniu działań wchodzących w zakres zastosowania prawa Unii, a także zasady dotyczące swobodnego przepływu takich danych. Przestrzeganie tych zasad podlega kontroli niezależnych organów; (3) Zasady przyjęte na podstawie niniejszego artykułu pozostają bez uszczerbku dla zasad szczególnych przewidzianych w artykule 39 Traktatu o Unii Europejskiej. Wersje skonsolidowane Traktatu o Unii Europejskiej i Traktatu o funkcjonowaniu Unii Europejskiej (Dz. Urz. UE C 326 z 26.10.2012 r., s. 1).
[2] Dz. Urz. UE L 119 z dn. 4.5.2016r., s. 1–88.
[3] Dz. Urz. UE L 295 z 21.11.2018 r., s. 39–98.
[4] Dz. Urz. UE L 119 z 4.5.2016 r., s. 89–131.
[5] Dz. Urz. UE L 8 z 12.1.2001 r., s. 1–22.
[6] Dz. Urz. UE L 281 z 23.11.1995 r., s. 31–50.
[7] Dz.Urz. UE L 135 z 24.5.2016 r., s. 53–114.
[8] Dz. Urz. UE L 261 z 6.8.2004 r., s. 24–27.

ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania[9], (4) dyrektywa 2001/20/WE Parlamentu Europejskiego i Rady z dnia 4 kwietnia 2001 r. w sprawie zbliżania przepisów ustawowych, wykonawczych i administracyjnych państw członkowskich, odnoszących się do wdrożenia zasady dobrej praktyki klinicznej w prowadzeniu badań klinicznych produktów leczniczych, przeznaczonych do stosowania przez człowieka[10], (5) dyrektywa 2002/58/WE z dnia 12 lipca 2002 w sprawie przetwarzania danych osobowych oraz ochrony prywatności w sektorze komunikacji elektronicznej[11], (6) dyrektywa Komisji 2005/28/WE z dnia 8 kwietnia 2005 r. ustalająca zasady oraz szczegółowe wytyczne dobrej praktyki klinicznej w odniesieniu do badanych produktów leczniczych przeznaczonych do stosowania u ludzi, a także wymogi zatwierdzania produkcji oraz przywozu takich produktów[12];

5) Normy krajowe konstytucyjne na przykładzie Polski: (1) art. 47 Konstytucji RP[13], (2) art. 51 Konstytucji RP[14];
6) Normy krajowe rangi ustawowej i wykonawcze (*lex generali*) na przykładzie Polski: (1) ustawa z 10 maja 2018 o ochronie danych osobowych[15], (2) ustawa z dnia 9 maja 2018 r. o przetwarzaniu danych dotyczących przelotu pasażera[16], (3) ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości[17], (4) ustawa z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania 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)[18], (5) rozporządzenie Rady Ministrów z dnia 14 stycznia 2019 r. w sprawie wysokości wynagrodzenia członków Rady do Spraw Ochrony Danych Osobowych oraz liczby jej posiedzeń w roku kalendarzowym[19], (6) rozporządzenie Rady Ministrów z 20 marca 2019 r. w sprawie wzoru legitymacji służbowej pracownika Urzędu Ochrony Danych Osobowych[20], (7) rozporządzenie

[9] Dz. Urz. UE L 119 z 4.5.2016 r., s. 132–149.
[10] Dz. Urz. UE L 121 z 1.5.2001 r., s. 34–44.
[11] Dz. Urz. UE L 201 z 31.07.2002 r., s. 37–47.
[12] Dz. Urz. UE L 91 z 9.4.2005 r., s. 13–19.
[13] Każdy ma prawo do życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym (Dz.U. z 1997 r., Nr 78, poz. 483 z późn. zm).
[14] (1) Nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jej osoby; (2) Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym; (3) Każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych. Ograniczenie tego prawa może określić ustawa; (4) Każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą (Dz.U. z 1997 r., Nr 78, poz. 483 z późn. zm). Na temat granic inwigilacji zob. wyrok TK z 30.07.2014, sygn. K 23/11, OTK-A 2014, nr 7, poz. 80. Szerzej na temat niejawnych metod pozyskiwania informacji o obywatelach zob. A. Rogala-Lewicki, *Classified methods of collecting information on citizens. Comparative legal study of invigilation in Poland*, Studium Europy Środkowej i Wschodniej, Nr 14/2020.
[15] Dnia 30 sierpnia 2019 r opublikowano Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej w sprawie ogłoszenia jednolitego tekstu ustawy o ochronie danych osobowych (t.j. Dz.U. z 2019 r. poz. 1781).
[16] Dz.U. 2019 r., poz. 1783.
[17] Dz.U. 2019 r., poz. 125.
[18] Dz.U. 2019 r., poz. 730.
[19] Dz.U z 2019 r., poz. 164.
[20] Dz.U. z 2019 r. poz. 697.

Prezesa Rady Ministrów z dnia 31 maja 2019 r. w sprawie trybu i sposobu realizacji zadań przez inspektora ochrony danych[21];

7) Nowelizacje ustawy z 10 maja 2018 r. o ochronie danych osobowych[22];
8) Normy krajowe rangi ustawowej i wykonawcze (*lex generali*) do wejścia w życie rozporządzenia 2016/679 na przykładzie Polski: (1) ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[23], (2) rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r., w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych[24], (3) rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 22 kwietnia 2004 r. w sprawie wzorów imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych[25], (4) rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 11 maja 2011 r. zmieniające rozporządzenie w sprawie wzorów imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych[26], (5) rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych[27], (6) rozporządzenie Ministra Administracji i Cyfryzacji z dnia 10 grudnia 2014r. w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji[28], (7) rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych[29], (8) rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji[30], (9) rozporządzenie Prezydenta Rzeczypospolitej Polskiej z dnia 19 listopada 2015 r. zmieniające rozporządzenie w sprawie nadania statutu Biuru Generalnego Inspektora Ochrony Danych Osobowych[31];
9) Nowelizacje ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[32];

[21] Dz.U. 2019 poz. 1041.
[22] (1) ustawa z dnia 3 lipca 2018 r. – Przepisy wprowadzające ustawę – Prawo o szkolnictwie wyższym i nauce (Dz.U. 2018 poz. 1669), (2) ustawa z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania 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 (Dz.U. 2019 poz. 730).
[23] Dz. U. z 2016 r., poz. 922.
[24] Dz.U. z 2004 r. nr 100, poz. 1024.
[25] Dz.U. z 2004 r. nr 94, poz. 923.
[26] Dz.U. z 2011 r. nr 103, poz. 601.
[27] Dz.U. z 2008 r. nr 229, poz. 1536.
[28] Dz.U. z 2014 r., poz. 1934.
[29] Dz.U. z 2015 r., poz. 719.
[30] Dz.U. z 2015 r., poz. 745.
[31] Dz.U. 2015 r., poz. 2020.
[32] (1) ustawa z dnia 26 listopada 1998 r. o finansach publicznych (Dz.U. 1998 nr 155 poz. 1014), (2) ustawa z dnia 23 grudnia 1999 r. o kształtowaniu wynagrodzeń w państwowej sferze budżetowej oraz o zmianie niektórych ustaw (Dz.U. 1999 nr 110 poz. 1255), (3) ustawa z dnia 21 stycznia 2000 r. o zmianie niektórych ustaw związanych z funkcjonowaniem administracji publicznej (Dz.U. 2000 nr 12 poz. 136), (4) ustawa z dnia 24 maja 2000 r. o Krajowym Rejestrze Karnym (Dz.U. 2000 nr 50 poz. 580), (5) ustawa z dnia 16 listopada 2000 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz.U. 2000 nr 116 poz. 1216), (6) Ustawa z dnia 11 kwietnia 2001 r. o zmianie ustawy o doradztwie podatkowym oraz niektórych innych ustaw (Dz.U. 2001 nr 42 poz. 474), (7) ustawa z dnia 11 kwietnia 2001 r. o rzecznikach patentowych (Dz.U. 2001 nr 49 poz. 509), (8) ustawa z dnia 25 sierpnia 2001 r. o zmianie ustawy o ochronie danych osobowych (Dz.U. z 2001 r. Nr 100, poz. 1087), (9) ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz.U. 2002 nr 74 poz. 676), (10) ustawa z dnia 30 sierpnia 2002 r. Przepisy wprowadzające ustawę – Prawo o ustroju sądów administracyjnych

10) Normy krajowe rangi ustawowej i wykonawcze (*lex specialis, sfera ochrony zdrowia)* na przykładzie Polski: (1) ustawa z dnia 5 grudnia 1996 r. o zawodzie lekarza i lekarza dentysty[33], (2) ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta[34] , (3) ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia[35], (4) rozporządzenie Ministra Zdrowia z dnia 6 czerwca 2013 r. w sprawie Systemu Ewidencji Zasobów Ochrony Zdrowia[36], (5) rozporządzenie Ministra Zdrowia z dnia 6 kwietnia 2020 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania[37].
11) Normy krajowe wykonawcze (*lex specialis, sfera bezpieczeństwa lotów)* na przykładzie Polski: (1) rozporządzenie Ministra Spraw Wewnętrznych z dnia 24 października 2012 r. w sprawie wymagań technicznych i organizacyjnych dotyczących przekazywania Straży Granicznej informacji przez przewoźników lotniczych[38], (2) rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 22 maja 2018 r. w sprawie określenia protokołów i formatów danych wykorzystywanych przez przewoźników lotniczych w celu przekazywania danych PNR do Krajowej Jednostki do spraw Informacji o Pasażerach[39], (3) rozporządzenie Rady Ministrów z dnia 30 maja 2018 r. w sprawie przetwarzania danych dotyczących przelotu pasażera przez Krajową Jednostkę do spraw Informacji o Pasażerach[40].

Od 25 maja 2018 roku nowy system opiera się przede wszystkim na treści 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), oraz implementowanych do polskiego prawa krajowego norm dyrektywy

i ustawę – Prawo o postępowaniu przed sądami administracyjnymi (Dz.U. 2002 nr 153 poz. 1271), (11) ustawa z dnia 23 stycznia 2004 r. Ordynacja wyborcza do Parlamentu Europejskiego (Dz.U. 2004 nr 25 poz. 219), (12) ustawa z dnia 22 stycznia 2004 r. o zmianie ustawy o ochronie danych osobowych oraz ustawy o wynagrodzeniu osób zajmujących kierownicze stanowiska państwowe (Dz.U. 2004 nr 33 poz. 285), (13) ustawa z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz.U. 2006 nr 104 poz. 708), (14) ustawa z dnia 9 czerwca 2006 r. Przepisy wprowadzające ustawę o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz.U. 2006 nr 104 poz. 711), (15) ustawa z dnia 24 sierpnia 2007 r. o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym (Dz.U. 2007 nr 165 poz. 1170), (16) ustawa z dnia 24 sierpnia 2007 r. o zmianie niektórych ustaw w związku z członkostwem Rzeczypospolitej Polskiej w Unii Europejskiej (Dz.U. 2007 nr 176 poz. 1238), (17) ustawa z dnia 12 lutego 2010 r. o zmianie ustawy o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Systemie Informacji Wizowej i ustawy o ochronie danych osobowych (Dz.U. 2010 nr 41 poz. 233), (18) ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. 2010 nr 182 poz. 1228), (19) ustawa z dnia 29 października 2010 r. o zmianie ustawy o ochronie danych osobowych oraz niektórych innych ustaw (Dz.U. 2010 nr 229 poz. 1497), (20) ustawa z dnia 16 września 2011 r. o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej, państw trzecich, agencjami Unii Europejskiej oraz organizacjami międzynarodowymi (Dz.U. 2011 nr 230 poz. 1371), (21) ustawa z dnia 7 listopada 2014 r. o ułatwieniu wykonywania działalności gospodarczej (Dz.U. 2014 poz. 1662), (22) ustawa z dnia 10 lipca 2015 r. o zmianie ustawy o prokuraturze, ustawy o wykonywaniu mandatu posła i senatora, ustawy o ochronie danych osobowych, ustawy o Instytucie Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu, ustawy o Rzeczniku Praw Dziecka oraz ustawy – Prawo o ustroju sądów powszechnych (Dz.U. 2015 poz. 1309), (23) ustawa z dnia 22 grudnia 2015 r. o zmianie ustawy o działach administracji rządowej oraz niektórych innych ustaw (Dz.U. 2015 poz. 2281), (23) ustawa z dnia 11 lutego 2016 r. o pomocy państwa w wychowywaniu dzieci (Dz.U. 2016 poz. 195), (24) ustawa z dnia 18 marca 2016 r. o zmianie ustawy o Rzeczniku Praw Obywatelskich oraz niektórych innych ustaw (Dz.U. 2016 poz. 677), (25) ustawa z dnia 8 grudnia 2017 r. o Służbie Ochrony Państwa (Dz.U. 2018 poz. 138), (26) ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz.U. 2018 poz. 723).

[33] Dz.U. z 1997 r., Nr 28 poz. 152.
[34] Dz.U. z 2009 r., Nr 52 poz. 417.
[35] Dz.U. z 2011 r. Nr 113, poz. 657.
[36] Dz.U. z 2013 r., poz. 671.
[37] Dz.U. z 2020 r., poz. 666.
[38] Dz.U. z 2012 r., poz. 1249.
[39] Dz.U. z 2018 r., poz. 1012.
[40] Dz.U. z 2018 r., poz. 1148.

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 oraz krajowych regulacji uzupełniających.

Przywołane przepisy, występujące w hierarchii normatywnej norm międzynarodowo-prawnych oraz konstytucyjnych a obowiązujące do czasu wejścia w życie RODO uległy modyfikacji w drodze kolejnych nowelizacji dotykających sfery ochrony danych osobowych, względnie anulacji, jak w przypadku ustawy o ochronie danych osobowych z 1997 roku oraz przepisów wykonawczych do niej. W obliczu powyżej zaprezentowanych zastrzeżeń należy zwrócić uwagę na aspekt dynamiki zmian prawnych, w wyniku działań legislacyjnych. Zmiany wprowadzane do polskich przepisów po 2018 roku objęły ok. 140 aktów prawnych, w tym tak znaczących, jak: kodeks pracy, prawo ubezpieczeniowe, prawo bankowe, przepisy o statystyce publicznej, ustawy traktujące o ochronie zdrowia czy działalności kulturalnej.

REFORMY 1997–2018

Wybrane zmiany w prawie ochrony danych osobowych w Polsce – przegląd na dwudziestolecie system

Mając na uwadze fakt, iż czas wejścia w życie dużej unijnej rekonstrukcji systemu ochrony danych osobowych zbiegł się w czasie z dwudziestoleciem polskiego systemu prawnego, który w 2017 roku obchodził swoje dwudziestolecie[41] – nie można nie zauważyć, iż stanowi to doskonały asumpt do zaprezentowania wybranych zmian prawnych dokonywanych na przestrzeni lat. Sfera ochrony danych osobowych jest regulowana na wielu płaszczyznach normatywnych: w prawie międzynarodowym[42], w prawie europejskim (wspólnotowym, unijnym)[43], w prawie krajowym na różnych jego poziomach (konstytucyjnym, ustawowym i wykonawczym)[44] jako prawo generalne, oraz sektorowe. Niemniej punktem odniesienia dla adresatów norm w zakresie ochrony danych osobowych w Polsce od 1997 roku jest ustawa o ochronie danych osobowych – i to jej ewolucja musi stanowić główny nurt rozważań w zakresie przeglądu na dwudziestolecie systemu.

Definicja danych osobowych

Po pierwsze prawa i obowiązki w zakresie ochrony danych osobowych aktywizują się w sytuacji przetwarzania danych osobowych. Definicje przetwarzania zawarte w prawie międzynarodowym i europejskim mimo, że nie są identyczne to prezentują bliskość znaczeniową[45]. I tak odpowiednio zgodnie z Konwencja nr 108 „automatyczne przetwarzanie" oznacza następujące operacje wykonywane w całości lub części przy pomocy metod zautomatyzowanych: rejestrowanie danych, z zastosowaniem do nich operacji logicznych i/albo arytmetycznych, ich modyfikowanie, usuwanie, odzyskiwanie lub rozpowszechnianie. RODO widzi „przetwarzanie danych osobowych" jako operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych

[41] Szerzej zob. *Prawna ochrona danych. Uzasadnienie projektu ustawy przyjętej przez Radę Ministrów 13 sierpnia 1996r.*, Przegląd Rządowy 1996, nr 10
[42] Zob. B. Banaszak, *Prawo do ochrony danych osobowych w Polsce* [w:] *O prawach człowieka. W podwójną rocznicę Paktów*, red. T. Jasudowicz, C. Mik, Księga Pamiątkowa w hołdzie Profesor Annie Michalskiej, Wyd. Dom Organizatora TNOiK, Toruń 1996, str. 249–256.
[43] Zob. A. Mednis *Ochrona danych osobowych w Konwencji Rady Europy i Dyrektywie Unii Europejskiej*, Państwo i Prawo 1996 r. nr 6, s. 29–41. Por. *Biała Księga. Polska – Unia Europejska. Ochrona danych osobowych*, red. J. Barta, R. Markiewicz, Opracowania i Analizy. Seria: Prawo, Zeszyt 32, Urząd Rady Ministrów, Biuro Pełnomocnika Rządu ds. Integracji Europejskiej oraz Pomocy Zagranicznej, Warszawa 1995.
[44] Zob. *Ochrona danych osobowych w Polsce i w Niemczech – koncepcje, praktyka, polityka*, Materiały z Konferencji z dn. 10–11.X.1996 r., Fundacja im. Friedricha Naumanna Przedstawicielstwo w Polsce, Wydział Prawa Uniwersytetu Wrocławskiego.
[45] Szerzej zob. J. Borecka, *Geneza prawnej ochrony danych osobowych i pojęcie danych osobowych*, Zeszyty Naukowe Instytutu Administracji Akademii im. Jana Długosza w Częstochowie 2006, nr 4, s. 5–14.

osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak 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[46].

Po drugie owe przetwarzanie dotyczy tylko wybranych informacji, które są danymi osobowymi w rozumieniu ustawowym. Te są definiowane jako wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest ta, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne[47]. Konwencja Nr 108 Rady Europy w art. 2 określa dane osobowe mianem każdej informacji dotyczącej osoby fizycznej o określonej tożsamości lub dającej się zidentyfikować. Cechą wyróżniającą dane osobowe od innych informacji dotyczących osób jest tzw. brak anonimowości. Z danymi osobowymi tzw. niezależny obserwator ma do czynienia tak długo, jak długo jest w stanie ustalić tożsamość jednostki, której dane dotyczą. Informacją o charakterze osobowym jest nie tylko taka informacja, która dotyczy konkretnej osoby (fr. *identifiée*), ale również takiej, której tożsamość można ustalić (fr. *identifiable* – dosłownie identyfikowalna) na podstawie innych udostępnionych danych[48].

Należy zauważyć, że charakter osobowy danych nie może zostać z góry przypisany żadnej kategorii danych[49]. Przesądza o tym zwrot „wszelkie informacje" zawarty w definicji danych osobowych. Zakres znaczeniowy pojęcia „informacja" powinien obejmować nie tylko znaki językowe, lecz także inne okoliczności towarzyszące znakom językowym lub nawet w pełni dane pozajęzykowe[50]. Dane osobowe mogą więc stanowić komunikaty wyrażone i zapisane w jakikolwiek sposób, niezależnie od sposobu, zakresu i swobody ich udostępniania, jak i niezależnie od sposobu ich pozyskania i przybierać formę zdjęcia, filmu, grafiki, zarejestrowanego głosu. Przykładowo dane wrażliwe – biometryczne są identyfikowane poprzez

[46] Ustawa z 1997 roku „przetwarzanie" rozumiała jako wykonywanie jakiekolwiek operacji na danych osobowych, w szczególności takich jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, w tym tych, które realizuje się w systemach informatycznych. Zob. odpowiednio art. 2 Konwencji Nr 108 o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych podpisana w Strasburgu dn. 28 stycznia 1981 r. (ogłoszona D.n. 85–1203, 15.11.1985, JO 20.11.1985. weszła w życie 1.10.1985); art. 4 pkt 2 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 (Dz. Urz. UE L 119 z dn. 4.05.2016, s. 1–88); art. 7 pkt 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 1997 nr 133 poz. 883 z późn. zm.).

[47] Art. 6 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2016 r., poz. 922).

[48] Aby stwierdzić, czy dana osoba fizyczna jest możliwa do zidentyfikowania, należy wziąć pod uwagę wszelkie rozsądnie prawdopodobne sposoby (w tym wyodrębnienie wpisów dotyczących tej samej osoby), w stosunku do których istnieje uzasadnione prawdopodobieństwo, iż zostaną wykorzystane przez administratora lub inną osobę w celu bezpośredniego lub pośredniego zidentyfikowania osoby fizycznej. Aby stwierdzić, czy dany sposób może być z uzasadnionym prawdopodobieństwem wykorzystany do zidentyfikowania danej osoby, należy wziąć pod uwagę wszelkie obiektywne czynniki, takie jak koszt i czas potrzebne do jej zidentyfikowania, oraz uwzględnić technologię dostępną w momencie przetwarzania danych, jak i postęp technologiczny. Zasady ochrony danych nie powinny więc mieć zastosowania do informacji anonimowych, czyli informacji, które nie wiążą się ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną. Motyw 26 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 (Dz. Urz. UE L 119 z dn. 4.05.2016, s. 1–88).

[49] Sposób wykorzystania danych osobowych (aspekt funkcjonalny) ma istotne znaczenie. Użycie danych osobowych wyłącznie w celu identyfikacji osoby, która złożyła oświadczenie woli w imieniu osoby prawnej, pozwala przyjąć, że dopóki dane osobowe człowieka są używane zgodnie z regułami społecznymi, nie można mówić ani o bezprawności. Przetwarzanie informacji o osobach fizycznych sprawujących funkcję organów osób prawnych nie może być uznane za działanie bezprawne dopóki, dopóty przetwarzanie takie odbywa się wyłącznie w celu i zakresie niezbędnym do prawidłowej identyfikacji tychże jako pełniących funkcję organów. Zob. wyrok SA w Gdańsku z 15.3.1996 r., I ACR 33/96, OSA 1996, Nr 7–8, poz. 31). Por. A. Mednis, *Ochrona danych osobowych w Konwencji Rady Europy i Dyrektywie Unii* Europejskiej, Państwo i Prawo 1996 r. nr 6, s. 35.

[50] A. Drozd, *Ustawa o ochronie danych osobowych. Komentarz. Wzory pism i przepisy*, Lexis Nexis, Warszawa 2008, s. 41.

linie papilarne, cechy twarzy, geometria ręki, czy cechy źrenicy. Nie jest zatem możliwe aprioryczne ustalenie katalogu informacji, uznanych za mające charakter danych osobowych. Normodawca wprowadza kategorię danych osobowych zwykłych oraz wrażliwych (sensytywnych), przewidując dla tych drugich wyższy poziom ochrony i bezpieczeństwa.

TABELA 1 Dane osobowe zwykłe

nazwiska i imiona	imiona rodziców	data urodzenia	miejsce urodzenia
adres zamieszkania lub pobytu	numer ewidencyjny PESEL	Numer Identyfikacji Podatkowej	miejsce pracy
zawód	wykształcenie	seria i numer dowodu osobistego	numer telefonu

Źródło: opracowanie własne na podstawie ustawy z dnia 29 sierpnia 1999 roku o ochronie danych osobowych (Dz.U. 1997 nr 133 poz. 883 z późn. zm.)

TABELA 2 Dane osobowe zwykłe, tzw. inne dane

adres IP komputera	adres poczty elektronicznej	numer rachunku bankowego
numer formularza rekrutacyjnego do projektu	imię i nazwisko oraz telefon kontaktowy do osoby, którą należy powiadomić w razie wypadku	

Źródło: opracowanie własne na podstawie ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz.U. 1997 nr 133 poz. 883 z późn. zm.)

W ustawie z 1997 roku, odmiennie niż w przypadku tzw. danych osobowych zwykłych, katalog danych osobowych wrażliwych był zamknięty i wynikał wprost z art. 27 ust. 1 ustawy, obejmując takie informacje jak: (a) pochodzenie rasowe/etniczne, (b) poglądy polityczne, (c) przekonania religijne i filozoficzne, (d) przynależność wyznaniowa, partyjna, związkowa, (e) stan zdrowia, (f) kod genetyczny, (g) nałogi, (h) życie seksualne. Dane sensytywne obejmują też dane dotyczące: skazań, mandatów karnych, orzeczeń o ukaraniu, innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym[51].

[51] W polskim systemie prawnym istnieje legalna definicja danych osobowych zwykłych, która opiera się na zamkniętym katalogu informacji. I tak, zgodnie z ustawą o funduszach inwestycyjnych, danymi osobowymi są: imiona i nazwisko, data i miejsce urodzenia, adres zamieszkania, a w przypadku obywateli Rzeczypospolitej Polskiej także numer PESEL. Zob. art. 2 pkt 33 ustawy z 27 maja 2004 roku o funduszach inwestycyjnych (t.j. Dz.U. z 2021 r., poz. 605).

Należy zauważyć, iż ostatecznie obowiązująca definicja (na koniec obowiązywania ustawy) była wynikiem nowelizacji ustawy dokonanych w 2001 roku[52] oraz w 2004 roku[53]. W pierwotnym brzmieniu definicja za dane osobowe uznawała każdą informację dotyczącą osoby fizycznej, pozwalającą na określenie tożsamości tej osoby. Taka redakcja przepisu spotkała się po pierwsze z wykładnią judykatury potwierdzającą sprzeczność definicji z wersją znajdującą wyraz w dyrektywie 95/46 WE. W oparciu o definicję danych osobowych w pierwotnym brzmieniu Naczelny Sąd Administracyjny uznał, że przedmiotem ochrony ustawy nie są wszystkie dane o osobach fizycznych lecz jedynie tzw. dane identyfikujące[54], a więc przykładowo: imię, nazwisko, adres, PESEL, NIP. W konsekwencji definicja ustawowa spotkała się z krytyką doktryny i nauki prawa wskazującej, że ustawa uznawała dane osobowe wyłącznie tzw. dane identyfikacyjne, w sytuacji gdy za dane osobowe powinny zostać uznane wszelkie informacje, jeżeli tylko możliwe jest ich odniesienie do konkretnej osoby[55].

Udostępnianie danych osobowych

Zagadnieniem podlegającym transformacjom normatywnym była kwestia udostępniania danych osobowych, która od samego początku obowiązywania ustawy z 1997 roku, stanowiła przedmiot kontrowersji i sporów prawnych. 7 marca 2011 roku weszła w życie nowelizacja[56] przepisów ustawy o ochronie danych osobowych uchylająca przepis art. 29 ustawy, który do tej pory określał zasady udostępniania danych osobowych[57].

Początkowo ustawodawca wyróżnił dwie postaci udostępniania danych: (1) w celu włączenia do zbioru danych, (2) w celu innym niż do włączenia do zbioru danych osobowych[58]. Rozróżnienie to nie w każdym przypadku opierało się na wystarczająco jasnych kryteriach – budząc od początku obowiązywania ustawy szereg wątpliwości. Pojęcie „uprawniony" do otrzymania danych na podstawie przepisów oznaczało, że z normy powszechnej wyraźnie wynikać musiało prawo gromadzenia danych, w tym żądania ich udostępnienia.

---

[52] Art. 6 ustawy otrzymał wtedy następujące brzmienie. W rozumieniu ustawy za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań. Zob. ustawa z dnia 25 sierpnia 2001 r. o zmianie ustawy o ochronie danych osobowych (Dz.U. z 2001 r. Nr 100, poz. 1087). Szerzej por. W. Zimny, *Praktyczne skutki nowelizacji ustawy o ochronie danych osobowych z dnia 25 sierpnia 2001 r.*, ODO 2001, nr 21.

[53] Ustawa z dnia 22 stycznia 2004 r. o zmianie ustawy o ochronie danych osobowych oraz ustawy o wynagrodzeniu osób zajmujących kierownicze stanowiska państwowe (Dz.U. 2004 nr 33 poz. 285). Przy tym należy mieć na uwadze, że w polskim systemie prawnym pojęcie danych osobowych pojawiło się po raz pierwszy w ustawie z 29 września 1994 r. o rachunkowości, nie mniej akt ten nie wprowadził definicji legalnej. Pierwszą definicją danych osobowych o charakterze pojęcia legalnego była ta zawarta w z art. 6 ustawy o ochronie danych osobowych, która wprost nawiązywała do definicji zawartej w art. 2 lit. a dyrektywy 95/46/WE. Do wejścia w życie RODO definicje zawarte w ustawach poszczególnych państw członkowskich były konstruowane w sposób znaczeniowo pokrewny. Od wejścia w życie RODO można oczywiście mówić o jednoznaczności. Zob. P. Litwiński, *Pojęcie danych osobowych w rozporządzeniu ogólnym o ochronie danych osobowych*, Informacja w administracji publicznej 2017, nr 3. Szerzej zob. A. Mednis, *Prawna ochrona danych osobowych,* wyd. SCHOLAR, Warszawa 1995; L. Kępa, *Ochrona danych osobowych*, Difin, Warszawa 2014, J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, Wolters Kluwer, Warszawa 2015.

[54] Wyrok NSA z dnia 17.11.2000 r. (II SA 1860/00, niepubl.).

[55] Zob. J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, Wolters Kluwer, Warszawa 2015, s. 383–384.

[56] Dokonana ustawą z dnia 29 października 2010 r. o zmianie ustawy o ochronie danych osobowych oraz niektórych innych ustaw (Dz. U. z 2010 r., nr 229, poz. 1497).

[57] Szerzej, zob. G. Sibiga, *Ochrona danych osobowych: zmiany w prawie w latach 2010–2012 oraz planowana reforma systemu*, Edukacja Prawnicza 2012, nr 10.

[58] Ustawa o ochronie danych osobowych rozróżniała w art. 29 ust. 1 i 2 dwie sytuacje udostępniania danych osobowych w celu innym, niż włączenie do zbioru danych: (1) udostępnianie danych podmiotom uprawnionym do ich otrzymania na podstawie przepisów prawa (art. 29 ust. 1) oraz (2) udostępnianie danych innym podmiotom (art. 29 ust. 2). W pierwszym przypadku, na administratorze danych spoczywał obowiązek udostępnienia danych, udostępnienie danych było tu więc obligatoryjne. W drugim przypadku natomiast udostępnienie miało charakter fakultatywny. Zob. art. 29 ustawy z dn. 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 1997 nr 133 poz. 883 z późn. zm.).

Analizując art. 29 ustawy w pierwotnym brzmieniu należy zastanowić się nad *ratio legis* stworzenia szczególnych przepisów regulujących zasady udostępniania danych osobowych w innym celu, niż włączenie do zbioru danych osobowych. W doktrynie zwrócono uwagę, że celem przyjęcia art. 29 ustawy było stworzenie ram prawnych dla otworzenia zasobów informacyjnych ze zbiorów danych administratorów z sektora publicznego. Zakresem przedmiotowym zastosowania art. 29 ustawy byli bowiem objęci wyłącznie administratorzy danych ze sfery prawa publicznego. Jednocześnie zakres podmiotowy regulacji uzasadniał wprowadzenie szczególnych przepisów właśnie w ustawie o ochronie danych osobowych. Odpowiednie normy, na podstawie których tworzone były poszczególne rejestry (zbiory danych), nie zawsze zawierały bowiem szczególne przepisy dotyczące udostępniania danych osobowych zawartych w tychże rejestrach. Stąd za celowe uznano wprowadzenie odpowiedniej regulacji na poziomie przepisów ustawy o ochronie danych osobowych[59].

Administrator danych nie mógł odmówić udostępnienia danych osobowych w sytuacji, w której wnioskodawca legitymował się stosownym przepisem, upoważniającym go do otrzymania takich danych[60]. Mając na uwadze powyższe, za kontrowersyjne należało uznać objęcie zakresem zastosowania art. 29 i 30 ustawy, pozostałych administratorów danych, tj. administratorów spoza sfery prawa publicznego, w wyniku zmiany przepisów ustawy dokonanej w 2004 roku. Tym bardziej, iż charakter przyjętego rozwiązania nie znajdował w pełni oparcia w przepisach prawa UE. Dyrektywa 95/46/WE nie zawierała żadnych przepisów dotyczących udostępniania danych osobowych[61]. Dane po nowelizacji z 2004 roku mogły być udostępniane również innym osobom i podmiotom. W takim przypadku, udostępnienie danych uwarunkowane było od spełnienia łącznie trzech przesłanek: (a) złożenia pisemnego, umotywowanego wniosku o udostępnienie danych, zawierającego informacje umożliwiające wyszukanie w zbiorze żądanych danych oraz wskazującego zakres i przeznaczenie danych[62], (b) wiarygodnego uzasadnienia potrzeby posiadania danych, (c) nienaruszenia praw i wolności osób, których dane dotyczą, wskutek udostępnienia ich danych osobowych[63].

---

[59] Zob. M. Sakowska-Baryła, *Udostępnianie danych osobowych na gruncie ustawy o ochronie danych osobowych* [w:] *Ochrona danych osobowych w Polsce z perspektywy dziesięciolecia*, red. P. Fajgielski, Wydawnictwo KUL, Lublin 2008, s. 103–126.

[60] Wskazać m.in. należy: (a) art. 34 ust. 2 ustawy o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu, nakazujący udostępnianie danych na rzecz imiennie upoważnionego funkcjonariusza, (b) art. 14 ust. 5 ustawy o Policji, nakazujący udostępnianie danych na rzecz imiennie upoważnionego policjanta, (c) art. 29 ust. 6 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, nakazujący udostępnianie danych na rzecz imiennie upoważnionego funkcjonariusza, (d) art. 9 ust. 1b ustawy o Straży Granicznej, nakazujący udostępnianie danych na rzecz upoważnionego funkcjonariusza, e) art. 6j ustawy o Służbie Celnej nakazujący udostępnianie danych na rzecz imiennie upoważnionego funkcjonariusza. T. Szewc, *Udostępnianie danych osobowych na wniosek*, Monitor Prawniczy 2006, nr 22, s. 12–30. Szerzej zob. T. Szewc, *Publicznoprawna ochrona informacji*, C.H. Beck, Warszawa 2007.

[61] X. Konarski, G. Sibiga, Zmiany *w ustawie o ochronie danych osobowych w świetle Dyrektywy 95/46/WE*, Monitor Prawniczy 2004, nr 12, s. 51.

[62] Zwraca uwagę fakt, iż złożenie wniosku o udostępnienie danych osobowych do dnia 1 maja 2004 roku, a więc do dnia wejścia w życie ustawy z 22 stycznia 2004 roku o zmianie ustawy o ochronie danych osobowych, powinno było nastąpić z wykorzystaniem specjalnego formularza, którego wzór określało obecnie nieobowiązujące rozporządzenie Ministra Spraw Wewnętrznych i Administracji. Wraz z utratą mocy obowiązującej przez rozporządzenie, usunięty został wymóg posługiwania się formularzem przy składaniu wniosku. Zob. rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 3 czerwca 1998 r. w sprawie określenia wzoru wniosku o udostępnienie danych osobowych, zgłoszenia zbioru danych do rejestracji oraz imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych (Dz.U. 1998 nr 80 poz. 522).

[63] Uchylony art. 29 ustawy: (1) w przypadku udostępniania danych osobowych w celach innych niż włączenie do zbioru, administrator danych udostępnia posiadane w zbiorze dane osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa. (2) dane osobowe, z wyłączeniem danych, o których mowa w art. 27 ust. 1, mogą być także udostępnione w celach innych niż włączenie do zbioru, innym osobom i podmiotom niż wymienione w ust. 1, jeżeli w sposób wiarygodny uzasadnią potrzebę posiadania tych danych, a ich udostępnienie nie naruszy praw i wolności osób, których dane dotyczą. (3) dane osobowe udostępnia się na pisemny, umotywowany wniosek, chyba że przepis innej ustawy stanowi inaczej. Wniosek powinien zawierać informacje umożliwiające wyszukanie w zbiorze żądanych danych oraz wskazywać zakres i przeznaczenie. (4) udostępnione dane osobowe można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione. Zob. art. 29 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 1997 nr 133 poz. 883).

Należy wyeksponować, iż administrator danych do którego skierowany został wniosek o udostępnienie danych, samodzielnie musiał ocenić, czy spełnione zostały warunki udostępnienia danych osobowych[64]. W pewnych przypadkach jednakże, na administratora danych nałożony został obowiązek odmowy udostępnienia danych. Przypadki te, w formie katalogu zamkniętego, wskazane zostały w art. 30 ustawy. I tak administrator odmawiał udostępnienia danych podmiotom innym niż wymienione w art. 29 ust. 1 jeżeli spowodowałoby to: (1) ujawnienie wiadomości zawierających informacje niejawne, (2) zagrożenie dla obronności lub bezpieczeństwa państwa, życia i zdrowia ludzi lub bezpieczeństwa i porządku publicznego, (3) zagrożenie dla podstawowego interesu gospodarczego lub finansowego państwa, (4) istotne naruszenie dóbr osobistych osób, których dane dotyczą, lub innych osób[65].

Pomimo istnienia enumeratywnie wskazanych, obligatoryjnych podstaw odmowy udostępnienia danych dopuszczenie podmiotów innych niż publiczne do tej procedury prawnej niewątpliwie naruszało pierwotną logikę przepisu. W uzasadnieniu projektu nowelizacji ustawy o ochronie danych osobowych stwierdzono, że nie istnieje dostateczna podstawa dla zróżnicowania pozycji administratorów danych w zakresie udostępniania danych osobowych ze względu na ich status[66]. Instytucja udostępnienia danych w takiej formie spotkała się z szeroką krytyką komentatorów, którzy zwracali uwagę na ułomność przepisu w tym kształcie, przywołując szereg zarzutów, w tym m.in. jak następuje:

a) istniały dostateczne przesłanki do rozróżnienia na administratorów z sektora publicznego i prywatnego w aspekcie udostępniania danych osobowych. Przesłanki te to z jednej strony konieczność bardziej restrykcyjnego regulowania dopuszczalności udostępniania danych osobowych przez podmioty ze sfery prawa publicznego, z drugiej strony natomiast – okoliczność gromadzenia danych osobowych przez tych administratorów na podstawie szczególnych przepisów prawa, niejednokrotnie w oparciu o obowiązek przekazywania danych przez osoby, których te dane dotyczą. Traktowanie w ten sam sposób podmiotów ze sfery prawa publicznego i prywatnego prowadzić mogło do nałożenia nadmiernych obowiązków na tych ostatnich[67];
b) wątpliwości budziła supozycja przepisu, by w przypadkach niemożliwych do jednoznacznego rozstrzygnięcia, administrator danych osobowych traktował je jako objęte zakresem art. 29 ustawy, tj. jako następujące nie w celu włączenia do zbioru danych. Postępowanie takie prowadziło do sytuacji, w której odbiorca danych, który nie potrafiła powołać się na żadną z podstaw prawnych przetwarzania danych osobowych spośród wymienionych w art. 23 ust. 1 ustawy, otrzymywał jednak dane osobowe w celu

[64] Zob. E. Kulesza, *Odmowa informacji nie zawsze uzasadniona*, Rzeczpospolita z 4.8.1998 r.
[65] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, Wolters Kluwer, Warszawa 2015, s. 612. Autorzy wskazują na taksatywny charakter wyliczenia przyczyn odmowy udostępnienia danych.
[66] Uzasadnienie do rządowego projektu ustawy o zmianie ustawy o ochronie danych osobowych, druk sejmowy Nr 2120, Sejm IV kadencji, s. 20), [dostęp: 15.05.2020].
[67] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona…*, Warszawa 2015, s. 597. Odmienny pogląd: A. Drozd, *Ustawa o ochronie danych osobowych. Komentarz. Wzory pism i przepisy*, Lexis Nexis, Warszawa 2008, s. 181.

włączenia do zbioru, zgodnie z procedurą określoną w art. 29 – i to bez wykazywania istnienia podstawy prawnej przetwarzania danych[68];

c) występowało potencjalne ryzyko udostępniania całego zbioru danych osobowych w oparciu o przesłankę włączenia (lub nie) do zbioru w sytuacji braku rozstrzygnięcia czy przepis odnosi się do całego zbioru czy dotyczy wyłącznie udostępniania pojedynczych danych – przy zastrzeżeniu, iż biorąc pod uwagę zasadę ochrony danych osobowych implikującą zawężenie ich udostępniania wydaje się, że przepis nie powinien znaleźć zastosowania do udostępniania danych w postaci zbioru danych[69];

d) udostępnianie danych na podstawie art. 29 ustawy było oderwane od tzw. „celu przetwarzania", o którym mówił przepis art. 26 ust. 1 pkt 2 ustawy, gdzie odbiorca danych osobowych związany był celem, dla jakiego dane osobowe zostały udostępnione, a wykroczenie poza ten cel oznaczało naruszenie jednego z obowiązków szczególnej staranności administratora danych osobowych. Cel, o którym mowa była w art. 26 ustawy, wprowadzał pewne wartości, których realizacji służyć miało przetwarzanie danych osobowych, podczas gdy cel udostępnienia danych w postaci ich włączenia lub nie do zbioru danych stanowił wyłącznie techniczny aspekt przetwarzania udostępnionych danych – pozbawiając *de facto* ochrony w oparciu o te wartości;

e) model udostępniania danych był regulacją niepełną, ze względu na funkcjonowanie w systemie prawnym szeregu szczególnych procedur udostępniania danych osobowych.

f) nowelizacja utrzymała w mocy art. 51 ustawy, który stypizował sankcję karną za udostępnienie danych osobom nieupoważnionym przez podmiot administrujący zbiorem danych lub podmiot zobowiązany do ochrony danych osobowych, co skutkowało sytuacją, w której istniała luka prawna w zakresie określenia podstawy udostępnienia danych – w kontekście ewentualnej odpowiedzialności karnej[70].

Uwagi należy uzupełnić o stanowisko prezentowane w doktrynie i orzecznictwie, gdzie ukształtowały się dwa odmienne stanowiska w zakresie stosowania przepisów Kodeksu postępowania administracyjnego do postępowań przed administratorami danych osobowych na postawie ustawy z 1997 roku. Zgodnie z pierwszym z nich, administrator danych prowadził postępowania – w tym postępowanie w przedmiocie udostępnienia danych osobowych – na podstawie przepisów KPA[71], w szczególności odmowa powinna przybrać formę decyzji

[68] T. Szewc, *Udostępnianie*..., s. 12–33. Autor wskazuje, że w takiej sytuacji administrator udostępniający dane powinien samodzielnie ustalić cel udostępnienia. Podobny pogląd: G. Sibiga, *Postępowanie w sprawach ochrony danych osobowych*, Dom Wydawniczy ABC, Warszawa 2003, s. 90

[69] A. Mednis A., *Ustawa o ochronie danych osobowych*, Wydawnictwo Prawnicze PWN, Warszawa 1999, s. 94. Odmienny pogląd: P. Litwiński, *Udostępnianie danych osobowych przez organy administracji samorządowej*, Państwo i Prawo 2006, nr. 1, s. 42–43.

[70] Komentatorzy na potrzeby dokonania oceny czy udostępnienie oraz przetwarzanie udostępnionych danych osobowych jest dopuszczalne, w stanie prawnym po nowelizacji, zalecali posiłkowanie się wprost przepisem art. 23 ustawy oraz zasadom ogólnym. Zob. R. Hamm, *Ochrona danych a prawo karne* [w:] O*chrona danych osobowych*, red. Wyrzykowski M., Instytut Spraw Publicznych, Warszawa 1999 r., str. 73–88. Szerzej por. *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, red. D. Lubasz, E. Bielak-Jomaa, Warszawa 2017; P. Fajgielski, *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2018; P. Litwiński, *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, Wyd. C.H. Beck, Warszawa 2017; *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, red. M. Sakowska-Baryła, Warszawa 2018.

[71] C. Martysz, *Zakres stosowania kodeksu postępowania administracyjnego w ustawie o ochronie danych osobowych* [w:] *Wolność informacji i jej granice*, red. G. Szpor, Katowice 1998, s. 33–38.

administracyjnej. Zgodnie z drugim stanowiskiem, do postępowań prowadzonych przez administratorów danych osobowych nie miały zastosowania przepisy KPA[72], albowiem żaden z przepisów ustawy o ochronie danych osobowych nie upoważniał administratora danych do prowadzenia postępowania i orzekania w trybie KPA[73].

Podsumowując, anulacja, w 2011 roku, art. 29 ustawy *de facto* usunęła cały szereg wątpliwości prawnych, które narosły głównie po nowelizacji przepisy z 2004 roku. Do czasu uchylenia ustawy z 1997 roku kwestię udostępniania danych oparto o zasady ogólne[74].

Powoływanie Administratora Bezpieczeństwa Informacji i rejestracja zbiorów danych

Administrator danych na mocy ustawy z 1997 roku zobowiązany był, z zastrzeżeniem wyjątków przewidzianych w ustawie, do rejestracji przy GIODO zbiorów danych występujących w jednostce organizacyjnej. 1 stycznia 2015 roku weszły w życie znowelizowane przepisy w zakresie obowiązku rejestracji zbiorów danych oraz powoływania Administratorów Bezpieczeństwa Informacji. Zmiany podyktowane były chęcią złagodzenia obciążeń dla administratorów danych w ramach pakietu ułatwień dla przedsiębiorców.

Zgodnie z nowymi zasadami z obowiązku zgłoszenia zbioru danych do rejestracji GIODO zwolnieni byli nie tylko – jak dotychczas – administratorzy zbiorów danych wymienionych w art. 43 ust. 1 ustawy, ale także ci administratorzy danych, u których został powołany i zgłoszony do GIODO, Administrator Bezpieczeństwa Informacji, który „wewnętrznie" prowadził dla administratora danych owy rejestr.

Zgodnie z art. 43 ust. 1a ustawy obowiązkowi rejestracji zbiorów danych osobowych, z wyjątkiem zbiorów zawierających dane wrażliwe, nie podlegał administrator danych, który powołał Administratora Bezpieczeństwa Informacji i zgłosił go Generalnemu Inspektorowi do rejestracji, z zastrzeżeniem art. 46e ust. 2 ustawy. Była to w rzeczywistości forma zachęty do wyznaczania Administratora Bezpieczeństwa Informacji w jednostkach organizacyjnych. Przy tym należy pamiętać, iż samo powoływanie ABI było fakultatywne a rozstrzygnięcie dotyczące jego powołania pozostawiono w gestii administratorów danych. Jednakże w przypadku niepowołania, jego zadania obowiązany był wykonywać administrator danych[75].

[72] Z. Goik, *Forma udostępnienia (odmowy udostępnienia) danych osobowych*, Radca Prawny 2000, nr 1, s. 43. Odnotować także należy stanowisko, zgodnie z którym udostępnienie danych powinno przybrać formę zaświadczenia, a do jego wydania stosuje się przepisy Działu VII KPA. Taki pogląd: W. Zimny, *Udostępnianie danych osobowych w trybie art. 29 ustawy o ochronie danych osobowych*, ODO 2000, nr 7, s. 5–7.

[73] Wyrok NSA z 19.4.2000 r. (II SA 2619/99, Wok. 2000, Nr 7, s. 43). Podobne stanowisko wyrażały Samorządowe Kolegia Odwoławcze: w Olsztynie (post. SKO w Olsztynie z 24.6.1999 r., SKO-511–27/99, OSS 2000, Nr 2, s. 74) we Wrocławiu (post. SKO we Wrocławiu z 8.2.2001 r., SKO 4521/1/01, OSS 2001, Nr 2, s. 38).

[74] (1) Udostępnianie danych osobowych może nastąpić po przedłożeniu wniosku o przekazanie lub udostępnienie informacji lub na podstawie ustnego wniosku (ale wtedy, gdy zachodzi konieczność niezwłocznego działania). (2) Udostępnianie danych osobowych może nastąpić tylko zgodnie z art. 23 ustawy. (3) Administrator Danych udostępniający dane osobowe, będzie mógł to uczynić m.in.: (a) na podstawie zgody osoby, której dane dotyczą (art. 23 ust. 1 pkt 1 Ustawy), (b) w celu realizacji umowy, której stroną jest osoba, której dane dotyczą (art. 23 ust. 1 pkt 3 Ustawy), (c) dla wypełnienia prawnie usprawiedliwionych celów przez siebie realizowanych np. marketing bezpośredni własnych produktów lub usług (art. 23 ust. 1 pkt 5 Ustawy). (4) Udostępnienie danych osobowych w oparciu o art. 23 ust. 1 pkt 5 Ustawy będzie mogło nastąpić, jeśli będzie ono niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez Administratora Danych albo podmiot, który ma je otrzymać. (5) Osoba upoważniona udostępniająca dane osobowe jest obowiązana zażądać od osoby uprawnionej pokwitowania udostępnienia danych zawierających informacje przekazane na podstawie pisemnego wniosku albo potwierdzenia faktu uzyskania wglądu w treść informacji. (6) Udostępnienie danych osobowych nie może naruszać praw i wolności osób, których udostępniane dane dotyczą. (7) Administrator Danych nadzoruje udostępnianie danych osobowych do innych podmiotów. Zob. art. 23 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 1997 nr 133 poz. 883 z późn. zm.).

[75] W przypadku powołania ABI, administrator danych, zgodnie z art. 46b ustawy, był obowiązany zgłosić ten fakt do rejestracji GIODO w terminie 30 dni od dnia jego powołania. Administratorzy Bezpieczeństwa Informacji zgłoszeni do rejestracji GIODO byli wpisywani do ogólnokrajowego, jawnego rejestru (art. 46c ustawy). Administrator danych, który zgłosi ABI do rejestracji zobowiązany był zgłaszać Generalnemu Inspektorowi każdą zmianę informacji

Powołanie ABI i zgłoszenie go GIODO do rejestracji, miało wpływ na zakres obowiązków dotyczących rejestracji zbiorów danych osobowych. W przypadku powołania prowadził on rejestr zbiorów danych osobowych (z wyjątkiem zbiorów danych wyłączonych z obowiązku zgłoszenia do rejestracji GIODO na podstawie art. 43 ust. 1 ustawy). Podkreślić jednak należy, iż nawet w przypadku powołania Administratora Bezpieczeństwa Informacji, obowiązkowi rejestracji podlegały zbiory, jeżeli były w nich przetwarzane dane szczególnie chronione, określone w art. 27 ust. 1 ustawy – czyli. tzw. dane wrażliwe (sensytywne). Dodać należy, iż katalog zwolnień zawarty w art. 43 ust. 1 ustawy został rozszerzony o pkt. 12, na podstawie którego z obowiązku rejestracji zbioru danych zwolnieni byli administratorzy przetwarzający dane w zbiorach, które nie były prowadzone z wykorzystaniem systemów informatycznych. Stąd przykładowo jeżeli w celu rejestrowania korespondencji wychodzącej i przychodzącej kierownik jednostki prowadził ewidencję korespondencji w formie papierowej i nie były w niej wpisywane dane wrażliwe, w rozumieniu ustawowym to zbiór danych np. pod nazwą: „ewidencja korespondencji", mógł być wyłączony z obowiązku rejestracyjnego.

Przepis art. 36a ust. 5 ustawy wprowadzał wymagania, które powinna spełniać osoba powołana na stanowisko Administratora Bezpieczeństwa Informacji, tj. mieć pełną zdolność do czynności prawnych, korzystać z pełni praw publicznych, posiadać odpowiednią wiedzę w zakresie ochrony danych osobowych, a także być niekarana za umyślne przestępstwo. W strukturze organizacyjnej ABI podlegać był powinien bezpośrednio kierownikowi jednostki organizacyjnej, osobie reprezentującej administratora danych. Jeżeli administrator danych zaniechał zgłoszenia Administratora Bezpieczeństwa Informacji do rejestracji, w rozumieniu przepisów przestawał on pełnić tę funkcję, a zadania ABI określone w art. 36a ust. 2 pkt 1 ustawy (z wyłączeniem obowiązku sporządzania sprawozdania) zobowiązany był wykonywać sam administrator, który jednocześnie ponosił odpowiedzialność za przestrzeganie przepisów.

Przekazywanie danych osobowych do państwa trzeciego

W ramach dużego pakietu nowelizacyjnego, którego przepisy weszły w życie w dniu 1 stycznia 2015 roku, zaktualizowano art. 48 ustawy, dopuszczając przekazywanie danych osobowych do państw trzecich, które nie zapewniają na swoim terytorium odpowiedniego poziomu ochrony danych osobowych, bez potrzeby uzyskania na to zgody wyrażonej przez Generalnego Inspektora Ochrony Danych Osobowych. Ustawodawca wprowadził ust. 2–5 do przepisu określając sytuacje, w których: (a) uzyskanie ww. zgody GIODO – w sytuacji spełnienia wymogu standardowej klauzuli umownej – nie było już wymagane, oraz (b) regulując tryb zatwierdzenia przez GIODO nowego instrumentu zapewniającego odpowiednie gwarancje praw i wolności osób, których dane dotyczą, tj. wiążących reguł korporacyjnych.

objętych zgłoszeniem powołania ABI w terminie 14 dni, a także jego odwołanie w terminie 30 dni, odpowiednio od dnia dokonania zmiany lub odwołania. Zgłoszenia powołania ABI do rejestracji Generalnemu Inspektorowi oraz zgłoszenia odwołania ABI należało dokonać przy użyciu wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji, które stanowiły załączniki do rozporządzenia Ministra Administracji i Cyfryzacji z dnia 10 grudnia 2014r. w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji (Dz.U. 2014 poz. 1934). Zob. art. 43 ust. 1a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 1997 nr 133 poz. 883 z późn. zm.).

TABELA 3 Zestawienie porównawcze rozdziału 7 ustawy z 1997 roku regulującego kwestie przekazywania danych osobowych do państwa trzeciego sprzed i po nowelizacji

Sprzed nowelizacji	*Po nowelizacji*
Art. 47. 1. Przekazanie danych osobowych do państwa trzeciego może nastąpić, jeżeli państwo docelowe daje gwarancje ochrony danych osobowych na swoim terytorium przynajmniej takie, jakie obowiązują na terytorium Rzeczypospolitej Polskiej. 2. Przepisu ust. 1 nie stosuje się, gdy przesłanie danych osobowych wynika z obowiązku nałożonego na administratora danych przepisami prawa lub postanowieniami ratyfikowanej umowy międzynarodowej. 3. Administrator danych może przekazać dane osobowe do państwa trzeciego, jeżeli: 1) osoba, której dane dotyczą, udzieliła na to zgody na piśmie, 2) przekazanie jest niezbędne do wykonania umowy pomiędzy administratorem danych a osobą, której dane dotyczą, lub jest podejmowane na jej życzenie, 3) przekazanie jest niezbędne do wykonania umowy zawartej w interesie osoby, której dane dotyczą, pomiędzy administratorem danych a innym podmiotem, 4) przekazanie jest niezbędne ze względu na dobro publiczne lub do wykazania zasadności roszczeń prawnych, 5) przekazanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, 6) dane są ogólnie dostępne. **Art. 48.** W przypadkach innych niż wymienione w art. 47 ust. 2 i 3 przekazanie danych osobowych do państwa trzeciego, które nie daje gwarancji ochrony danych osobowych przynajmniej takich, jakie obowiązują na terytorium Rzeczypospolitej Polskiej, może nastąpić po uzyskaniu zgody Generalnego Inspektora, pod warunkiem że administrator danych zapewni odpowiednie zabezpieczenia w zakresie ochrony prywatności oraz praw i wolności osoby, której dane dotyczą.	**Art. 47.** 1. Przekazanie danych osobowych do państwa trzeciego może nastąpić, jeżeli państwo docelowe zapewnia na swoim terytorium odpowiedni poziom ochrony danych osobowych. 1a. Odpowiedni poziom ochrony danych osobowych, o którym mowa w ust. 1, jest oceniany z uwzględnieniem wszystkich okoliczności dotyczących operacji przekazania danych, w szczególności biorąc pod uwagę charakter danych, cel i czas trwania proponowanych operacji przetwarzania danych, kraj pochodzenia i kraj ostatecznego przeznaczenia danych oraz przepisy prawa obowiązujące w danym państwie trzecim oraz stosowane w tym państwie środki bezpieczeństwa i zasady zawodowe. 2. Przepisu ust. 1 nie stosuje się, gdy przesłanie danych osobowych wynika z obowiązku nałożonego na administratora danych przepisami prawa lub postanowieniami ratyfikowanej umowy międzynarodowej, gwarantującymi odpowiedni poziom ochrony tych danych. 3. Administrator danych może jednak przekazać dane osobowe do państwa trzeciego, jeżeli: 1) osoba, której dane dotyczą, udzieliła na to zgody na piśmie; 2) przekazanie jest niezbędne do wykonania umowy pomiędzy administratorem danych a osobą, której dane dotyczą, lub jest podejmowane na jej życzenie; 3) przekazanie jest niezbędne do wykonania umowy zawartej w interesie osoby, której dane dotyczą, pomiędzy administratorem danych a innym podmiotem; 4) przekazanie jest niezbędne ze względu na dobro publiczne lub do wykazania zasadności roszczeń prawnych; 5) przekazanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą; 6) dane są ogólnie dostępne. **Art. 48.** 1. W przypadkach innych niż wymienione w art. 47 ust. 2 i 3 przekazanie danych osobowych do państwa trzeciego, które nie zapewnia na swoim terytorium odpowiedniego poziomu ochrony danych osobowych, może nastąpić po uzyskaniu zgody Generalnego Inspektora, wydanej w drodze decyzji administracyjnej, pod warunkiem że administrator danych zapewni odpowiednie zabezpieczenia w zakresie ochrony prywatności oraz praw i wolności osoby, której dane dotyczą. 2. Zgoda Generalnego Inspektora nie jest wymagana, jeżeli administrator danych zapewni odpowiednie zabezpieczenia w zakresie ochrony prywatności oraz praw i wolności osoby, której dane dotyczą, przez: 1) standardowe klauzule umowne ochrony danych osobowych, zatwierdzone przez Komisję Europejską zgodnie z art. 26 ust. 4 dyrektywy 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 lub 2) prawnie wiążące reguły lub polityki ochrony danych osobowych, zwane dalej „wiążącymi regułami korporacyjnymi", które zostały zatwierdzone przez Generalnego Inspektora zgodnie z ust. 3–5. 3. Generalny Inspektor zatwierdza, w drodze decyzji administracyjnej, wiążące reguły korporacyjne przyjęte w ramach grupy przedsiębiorców do celów przekazania danych osobowych przez administratora danych lub podmiot, o którym mowa w art. 31 ust. 1, do należącego do tej samej grupy innego administratora danych lub podmiotu, o którym mowa w art. 31 ust. 1, w państwie trzecim. 4. Generalny Inspektor przed zatwierdzeniem wiążących reguł korporacyjnych może przeprowadzić konsultacje z właściwymi organami ochrony danych osobowych państw należących do Europejskiego Obszaru Gospodarczego, na których terytorium mają siedziby przedsiębiorcy należący do grupy, o której mowa w ust. 3, przekazując im niezbędne informacje w tym celu. 5. Generalny Inspektor, wydając decyzję, o której mowa w ust. 3, uwzględnia wyniki przeprowadzonych konsultacji, o których mowa w ust. 4, a jeżeli wiążące reguły korporacyjne były przedmiotem rozstrzygnięcia organu ochrony danych osobowych innego państwa należącego do Europejskiego Obszaru Gospodarczego – może uwzględnić to rozstrzygnięcie.

Źródło: zestawienie na podstawie zmian ustawy z dnia 29 sierpnia 1999 r. o ochronie danych osobowych (Dz.U. 1997 nr 133 poz. 883 z późn. zm.)

Nowelizacja wprowadzała zasadę, zgodnie z którą przekazanie danych osobowych do państwa trzeciego mogło nastąpić, jeżeli państwo docelowe zapewniało na swoim terytorium odpowiedni poziom ochrony danych osobowych. Przed zmianą dopuszczalne było przekazanie danych do państwa trzeciego jeżeli zapewniało ono gwarancje ochrony danych osobowych na swoim terytorium przynajmniej takie, jakie obowiązują na terytorium RP.

Wprowadzona klauzula generalna: „odpowiedni poziom", nie była jednak pozostawiona swobodnej interpretacji. Ocena odbywać się była powinna z uwzględnieniem wszystkich okoliczności dotyczących operacji przekazania danych, w szczególności biorąc pod uwagę charakter danych, cel i czas trwania proponowanych operacji przetwarzania danych, kraj pochodzenia, kraj ostatecznego przeznaczenia danych oraz przepisy prawa obowiązujące w danym państwie trzecim, jak również stosowane w tym państwie środki bezpieczeństwa i zasady zawodowe. Niezmiennie administrator mógł przekazać dane do państwa trzeciego, jeżeli: (1) osoba, której dane dotyczą, udzieliła na to zgody na piśmie, (2) przekazanie było niezbędne do wykonania umowy pomiędzy administratorem danych a osobą, której dane dotyczą, lub było podejmowane na jej życzenie, (3) przekazanie było niezbędne do wykonania umowy zawartej w interesie osoby, której dane dotyczą, pomiędzy administratorem danych a innym podmiotem, (4) przekazanie było niezbędne ze względu na dobro publiczne lub do wykazania zasadności roszczeń prawnych, (5) przekazanie było niezbędne do ochrony żywotnych interesów osoby, której dane dotyczyło, (6) dane były ogólnie dostępne.

W pozostałych przypadkach przekazanie danych osobowych do państwa trzeciego, które nie zapewniało na swoim terytorium odpowiedniego poziomu ochrony danych osobowych, mogło nastąpić po uzyskaniu zgody Generalnego Inspektora, wydanej w drodze decyzji administracyjnej, pod warunkiem że administrator danych zapewnił odpowiednie zabezpieczenia w zakresie ochrony prywatności oraz praw i wolności osoby, której dane dotyczyły. Zgoda GIODO wyrażona w drodze decyzji administracyjnej nie była wymagana, jeżeli administrator danych zapewnił odpowiednie zabezpieczenie danych, poprzez: (a) standardowe klauzule umowne ochrony danych osobowych zatwierdzone przez Komisję Europejską[76], (b) prawnie wiążące reguły lub polityki ochrony danych osobowych, tzw. wiążące reguły korporacyjne[77].

[76] Standardowe klauzule umowne zatwierdzone przez Komisję Europejską zgodnie z art. 26 ust. 4 Dyrektywy 95/45/WE można było stosować w umowach z podmiotami z państw trzecich. Komisja Europejska wydała w tym czasie trzy decyzje w tym zakresie: (1) Decyzja Komisji 2001/497/WE w sprawie wzorcowych klauzul umownych w związku z przekazywaniem danych osobowych do państw trzecich na podstawie Dyrektywy 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. WE L 181/19 z 04.07.2001r.) z dnia 15 czerwca 2001 r. – wprowadzająca standardowe klauzule umowne mające zastosowanie do przekazywania danych osobowych do administratora danych w państwie trzecim; (2) Decyzja Komisji 2004/915/WE zmieniająca decyzję 2001/497/WE w zakresie alternatywnego zestawu standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich (Dz.Urz. WE L 385/19 z 29.12.2004r.) z dnia 27 grudnia 2004 r. – wprowadzająca zestaw alternatywnych klauzul umownych, które administrator danych może wykorzystać w przypadku przekazywania danych do innego administratora danych w państwie trzecim; (3) Decyzja Komisji 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 Parlamentu Europejskiego i Rady z dnia 5 lutego 2010 r. – wprowadzająca standardowe klauzule umowne mają zastosowanie do przekazywania danych osobowych w przypadku powierzenia przetwarzania danych osobowych w rozumieniu art. 31 polskiej ustawy o ochronie danych osobowych. Zob. A. Mednis, *Transgraniczny przepływ danych osobowych z polskiej perspektywy* [w:] *1998–2013. 15-lecie ustawy o ochronie danych osobowych*, Wydawnictwo Biura Generalnego Inspektora Ochrony Danych Osobowych, Warszawa 2013, s. 40. Zob też B. Fischer, *Ponadgraniczne przekazywanie danych osobowych – charakter prawny regulacji z uwzględnieniem uzupełniającej roli soft law* [w:] *Prywatność a ekonomia. Ochrona danych osobowych w obrocie gospodarczym*, red. A. Mednis Warszawa 2013, s. 81–90.

[77] Z kolei tzw. wiążące reguły korporacyjne, o których mowa w ust. 3 znowelizowanego przepisu dotyczyły podmiotów należących do tej samej grupy przedsiębiorców (tej samej grupy kapitałowej). Wiążące reguły korporacyjne mogły być stosowane po ich zatwierdzeniu przez GIODO (w drodze decyzji administracyjnej), po przeprowadzeniu nieobowiązkowych konsultacji z organami ochrony danych osobowych państw Europejskiego Obszaru Gospodarczego (państwa Unii Europejskiej oraz Islandia, Norwegia, Liechtenstein, na których terytorium mają siedziby przedsiębiorcy należący do ww. grupy).

Należy zaznaczyć, iż dokonanie modyfikacji w zakresie tzw. standardowych klauzul umownych pozwalających na przekazanie danych do państwa trzeciego bez konieczności uzyskania zgody GIODO, co do zasady pozbawiało tej konstrukcji prawnej przymiotu standardowych klauzul umownych ustanowionych decyzją Komisji Europejskiej, a tym samym wymagane było uprzednie uzyskanie zgody GIODO na przekazanie danych osobowych do państw trzecich, które nie zapewniały odpowiedniego poziomu ochrony danych.

Nie można stracić z pola widzenia faktu, iż znowelizowane przepisy art. 47 i 48 ustawy wprowadzały jedynie dodatkowe wymogi, które należało spełnić, w sytuacji przekazywania danych osobowych do państw trzecich. W przypadku kwalifikowanej formy przetwarzania danych, jaką było przekazanie danych do innego administratora danych, który miał siedzibę w państwie trzecim, zachodziła konieczność spełnienia jednej z przesłanek legalności przetwarzania danych, wymienionych w art. 23 ust. 1 lub art. 27 ust. 2 ustawy, w szczególności administrator danych musiał m.in. zapewnić, aby ich zakres był dopuszczalny w świetle powszechnie obowiązujących na terytorium RP przepisów prawa.

Uznanie za jednego Administratora Danych w sytuacji przetwarzania danych osobowych służących temu samemu interesowi publicznemu

Jedną z ostatnich zmian ustawy z 1997 roku, która weszła w życie jeszcze przed RODO, była zmiana przepisu art. 38 pkt 1 wprowadzona 1 kwietnia 2016 roku ustawą o pomocy państwa w wychowywaniu dzieci, potocznie zwana ustawą 500+. *W ustawie o ochronie danych osobowych wprowadzono następujące zmiany:*

a) w art. 23 po ust. 2 dodano ust. 2a w brzmieniu: „Podmioty, o których mowa w art. 3 ust. 1, uważa się za jednego administratora danych, jeżeli przetwarzanie danych służy temu samemu interesowi publicznemu",
b) w art. 31 po ust. 2 dodano ust. 2a w brzmieniu: „Nie wymaga zawarcia umowy między administratorem a podmiotem, o którym mowa w ust. 1, powierzenie przetwarzania danych, w tym przekazywanie danych, jeżeli ma miejsce między podmiotami, o których mowa w art. 3 ust. 1"[78].

Zmiany przepisów były o tyle istotne, że odnosiły się podstawowych zasad przetwarzania danych osobowych – pojęcia administratora danych oraz kwestii związanych z powierzeniem przetwarzania danych osobowych między organami państwowymi i samorządowymi[79]. Zmiany od razu wywołały szereg kontrowersji i wątpliwości interpretacyjnych. Należy wyeksponować, iż tuż po ich wejściu w życie, w Wystąpieniu do Generalnego Inspektora

Zob. B. Fischer, *Zasady transferu danych osobowych z Polski na przestrzeni 10 lat obowiązywania ustawy o ochronie danych osobowych* [w:] *10 lat ochrony danych osobowych w Polsce*, red. Fajgielski P., KUL, Lublin 2008, str. 127–140. Por. też. D. Lubasz, *Przekazywanie danych osobowych do państw trzecich w ogólnym rozporządzeniu o ochronie danych*, Monitor prawniczy 2016, nr 20; M. Krzysztofek, *Przekazywanie z UE do USA danych z komunikatów finansowych w systemie SWIFT*, Państwo i Prawo 2011, nr 7–8.

[78] Ustawa z dnia 11 lutego 2016 r. o pomocy państwa w wychowywaniu dzieci (t.j. Dz. U. z 2019 r. poz. 2407; z 2021 r. poz. 1162).

[79] *GIODO: ustawa 500 plus próbuje zmodyfikować podstawowe zasady przetwarzania danych osobowych*, https://samorzad.infor.pl/sektor/zadania/opieka_spoleczna/737744,GIODO-ustawa-500-plus-probuje-zmodyfikowac-podstawowe-zasady-przetwarzania-danych-osobowych.html, [dostęp: 27.04.2019].

Ochrony Danych Osobowych ws. ochrony danych osobowych w związku z realizacją programu Rodzina 500 plus z 30 marca 2016 roku, Rzecznik Praw Obywatelskich wyraził wątpliwości odnośnie realizacji prawa do prywatności oraz prawa do ochrony danych osobowych w przepisach ujawnionych w ustawie. RPO zaniepokoiły warunki nabywania praw do świadczenia wychowawczego oraz zasady przyznawania i wypłacania tego świadczenia. Rzecznik sygnalizował niezgodność przepisów dotyczących podmiotów publicznych będących współadministratorami danych z prawem unijnym. Wątpliwości wiązały się także z koniecznością rejestrowania przez gminy zbiorów danych u GIODO. „Niektóre dane zawarte w dokumentach dołączonych do wniosku osoby ubiegającej się o świadczenie wychowawcze mogły być uznane za dane wrażliwe, jak chociażby zaświadczenie o prowadzonym postępowaniu sądowym w sprawie o przysposobienie dziecka czy prawomocne orzeczenie sądu orzekające rozwód lub separację”[80]. Przetwarzanie danych wrażliwych przed zarejestrowaniem zbioru danych nie było przecież dopuszczalne.

Rzecznik Praw Obywatelskich wskazywał, że nie jest jasne, czy cel i zakres pozyskiwanych danych mogą być uznane za „niezbędne w demokratycznym państwie prawnym” i czy takie ograniczenie prawa do prywatności[81] będzie mogło być uznane za zgodne z art. 47 i art. 51 w zw. z art. 31 ust. 3 Konstytucji, m.in. formułując takie zarzuty[82] jak:

a) konieczność weryfikacji, czy wszystkie dane są niezbędne dla realizacji świadczenia (konieczność podawania szczegółowych informacji o dochodach, w tym również każdego członka rodziny, o niepełnosprawności, czy karalności – które to dane nie wydawały się niezbędne dla potwierdzenia prawidłowości ubiegania się o świadczenie);
b) sposób zasilania centralnego rejestru, a także zasady udostępniania danych innym podmiotom, w tym brak regulacji odnośnie trybu udostępniania informacji z rejestru centralnego, oznaczające brak adekwatności, przejrzystości i precyzyjności;
c) brak uregulowania okresu przechowywania danych osobowych przez organy właściwe i inne upoważnione podmioty oraz marszałków województw, a także brak uzasadnienia dla 10-letniego okresu przechowywania danych w rejestrze centralnym;
d) możliwość pisemnego upoważnienia przez właściwy organ kierownika „innej jednostki organizacyjnej gminy” lub innej osoby na wniosek m.in. kierownika „innej jednostki organizacyjnej gminy”, który nie wskazywał, kto dokładnie może mieć dostęp do danych osobowych;
e) możliwość weryfikacji faktu samotnego wychowywania dziecka w formie pełnego wywiadu środowiskowego, implikującego konieczność przetwarzania danych osobowych w zakresie szerszym, niż wskazywałby na to cel ustawy;

[80] *Wystąpienie do Generalnego Inspektora Ochrony Danych Osobowych ws. ochrony danych osobowych w związku z realizacją programu Rodzina 500 plus*, https://www.rpo.gov.pl/pl/content/wystapienie-do-giodo-ws-ochrony-danych-osobowych-w-zwiazku-z-realizacja-programu-500-plus, [dostęp: 27.04.2019].
[81] Szerzej na temat prawa do prywatności zob. *Prawo prywatności jako reguła społeczeństwa informacyjnego*, red. K. Chałubińska-Jentkiewicz, K. Kakareko, J. Sobczak, Warszawa 2017.
[82] Program 500+ a ochrona danych osobowych, https://blog-daneosobowe.pl/program-500-a-ochrona-danych-osobowych/, http://wartowiedziec.pl/polityka-spoleczna/30128-program-500-a-ochrona-danych-osobowych, [dostęp: 27.04.2020].

f) brak wymogu zebrania od beneficjentów programu 500+ oddzielnej zgody na przetwarzanie danych osobowych w celu wypłaty świadczeń, mimo że we wniosku ujawniane były dane wrażliwe.

W reakcji na wystąpienie Rzecznika Praw Obywatelskich, Generalny Inspektor Ochrony Danych Osobowych, zaprezentował, w swoim Komunikacie, swoje stanowisko odnośnie nowych regulacji. GIODO zadeklarował po pierwsze, że będzie interpretował, dodane przez art. 38 ustawy o pomocy państwa w wychowywaniu dzieci, przepisy art. 23 ust. 2a oraz art. 31 ust. 2a ustawy uwzględniając całokształt własnej wykładni, po drugie mając na względzie niezgodność konstrukcji prawnej przewidzianej w art. 23 ust. 2a z obowiązującym prawem europejskim – w tym zakresie będzie dążył do zmiany tego aktu prawnego[83]. Generalny Inspektor Ochrony Danych Osobowych podnosił m.in. następujące zarzuty:

a) „przyjęta w art. 38 pkt 1 ustawy o pomocy państwa w wychowywaniu dzieci nowelizacja ustawy o ochronie danych osobowych nie może zmieniać ogólnej zasady, na podstawie której każdy z administratorów odpowiada za realizację zadań we własnym, wyznaczonym właściwymi przepisami, i tym samym nie może być mowy o odpowiedzialności solidarnej, gdyż na gruncie prawa administracyjnego nie jest znana konstrukcja odpowiedzialności solidarnej, przy czym art. 23 ust. 2a ustawy nie może być traktowany w oderwaniu od przepisów szczególnych na podstawie których należy oceniać zakres odpowiedzialności oraz dopuszczalnego przetwarzania danych przez poszczególnych administratorów danych i podmioty przetwarzające dane;
b) przepisy ustawy o ochronie danych osobowych stanowiąc implementację *dyrektywy 95/46/WE* nie mogą być interpretowane w oderwaniu od wykładni norm prawa unijnego, co potwierdza orzecznictwo Trybunału Sprawiedliwości UE, w szczególności w przypadku niewłaściwej transpozycji dyrektywy możliwe jest bezpośrednie powoływanie się na jej przepisy przez jednostki występujące przed sądami, tymczasem w opinii GIODO wprowadzona zmiana stoi w sprzeczności z obowiązującym prawem unijnym, co skutkować może zarzutem błędnej transpozycji dyrektywy;
c) konstrukcja prawna pozycji administratora danych, czyli najważniejszego podmiotu w procesie przetwarzania danych, decydującego o celach i środkach przetwarzania danych osobowych, zarówno ze względu na ciążące na nim rozliczne obowiązki, jak i posiadane przez niego uprawnienia w procesie przetwarzania danych, musi być jednoznacznie zidentyfikowana, na co zwraca uwagę chociażby Grupa Robocza art. 29, która w Opinii 1/2010 w sprawie pojęć „administrator danych" i „przetwarzający", przyjętej w dniu 16 lutego 2010 r., wskazała, iż zamieszczona w prawie unijnym definicja administratora danych kładzie nacisk m.in. na aspekt o charakterze personalnym, tzn. administratorem danych może być: osoba fizyczna lub prawna, władza publiczna, agencja lub inny organ

[83] *Komunikat dotyczący nowelizacji ustawy o ochronie danych osobowych*, GIODO https://archiwum.giodo.gov.pl/560/id_art/9121, [dostęp: 27.04.2020].

– wobec powyższego wprowadzenie w miejsce ugruntowanej w obowiązującym prawie konstrukcji administratora danych koncepcji „jednego administratora" w odniesieniu do podmiotów wskazanych w art. 3 ust. 1 ustawy o ochronie danych osobowych (zgodnie z którą podmioty te łącznie stanowią jednego administratora), spowoduje dla samych administratorów trudności w praktycznym stosowaniu przepisu, nie wyłączając ich pełnej odpowiedzialności;

d) przyjęcie dopuszczalności powierzenia ustawowego danych osobowych z rezygnacją z wymogu zawarcia umowy powierzenia przetwarzania danych, jeżeli powierzenie ma miejsce między podmiotami, o których mowa w art. 3 ust. 1 ustawy (tj. organami państwowymi, organami samorządu terytorialnego oraz państwowymi i komunalnymi jednostkami organizacyjnymi) w kształcie po nowelizacji bez jednoczesnego stworzenia w tym zakresie odpowiednich gwarancji, w szczególności jasnego określenia zasad, na jakich to powierzenie ma mieć miejsce nie powinno się wiązać z obniżeniem poziomu ochrony tych danych i niespełnieniem szeregu warunków określanych do tej pory w umowach *ergo* jest niewystarczającą podstawą do powierzenia przetwarzania danych innemu podmiotowi i w tym sensie nadal powierzenie odbywać się powinno na zasadach ogólnych, tj. na podstawie umowy, o której mowa w art. 31 ust. 1 ustawy"[84].

Należy zgodzić się ze stanowiskiem, iż przed kolejnymi zakusami legislatora, system ODO w ramach 500+, uratował całkowicie nowy porządek prawny (RODO). Ustawa, po wejściu w życie RODO, została zaktualizowana, stanowiąc próbę dostosowania jej do wymogów rozporządzenia 2016/679 m.in. w zakresie przypisania procesu przetwarzania do administratora danych, okresu przechowywania informacji w rejestrze (okres 10 lat od dnia zaprzestania udzielania świadczenia wychowawczego, okres 10 lat od dnia ich udostępnienia z rejestru centralnego), pseudonimizacji danych, zabezpieczeń fizycznych, technicznych i organizacyjnych, spełnienia obowiązku informacyjnego[85], celu udostępnienia danych oraz podmiotów, którym dane są udostępniane (informacje zawarte w rejestrze centralnym zaczęto udostępniać w zakresie niezbędnym do realizacji ich zadań ustawowych), czy możliwości przeprowadzania audytów i kontroli[86]. Przy czym za cały czas aktualne uznać trzeba zastrzeżenia w zakresie

[84] *Komunikat dotyczący nowelizacji ustawy o ochronie danych osobowych*, GIODO, https://archiwum.giodo.gov.pl/560/id_art/9121, [dostęp: 27.04.2020].

[85] M. Topolewska, *500+ a RODO: Rodzice jednak muszą zostać poinformowani o przetwarzaniu danych osobowych*, https://prawo.gazetaprawna.pl/artykuly/1159736,przetwarzanie-danych-osobowych-a-500.html, [dostęp: 27.04.2020].

[86] Minister właściwy do spraw rodziny tworzy rejestr centralny obejmujący następujące informacje gromadzone na podstawie przepisów ustawy przez organy właściwe i wojewodów podczas realizacji zadań w zakresie świadczenia wychowawczego 1) dane dotyczące osób pobierających świadczenie wychowawcze, osób ubiegających się o świadczenie wychowawcze oraz dzieci, na które osoby te pobierają świadczenie wychowawcze lub ubiegają się o przyznanie tego świadczenia: (a) imię i nazwisko, (b) datę urodzenia, (c) adres miejsca zamieszkania, miejsce zamieszkania, (d) numer PESEL, (e) numer i serię dokumentu potwierdzającego tożsamość w przypadku osób, które nie posiadają numeru PESEL, (f) stan cywilny, (g) obywatelstwo, (h) stopień pokrewieństwa, (i) (uchylona) (ia) informacje o uczęszczaniu dziecka do szkół i placówek oświatowych, o których mowa w art. 3 ust. 1 pkt 1 ustawy z dnia 15 kwietnia 2011 r. o systemie informacji oświatowej (Dz. U. z 2019 r. poz. 1942), okresie uczęszczania, typie lub rodzaju instytucji oraz nazwie i adresie siedziby instytucji, do której dziecko uczęszcza, (ib) informacje o prawie do świadczeń opieki zdrowotnej, (ic) (uchylona), (j) liczbę i wysokość wypłaconych świadczeń, (k) płeć, (l) (uchylona), (m) organ, do którego złożono wniosek, oraz datę złożenia wniosku, (n) organ, który przyznał świadczenie, datę przyznania świadczenia oraz numer sprawy, (o) okres, na jaki świadczenie zostało przyznane; (2) wartości udzielonych świadczeń. Informacje, o których mowa w ust. 2, są przetwarzane przez ministra właściwego do spraw rodziny i wojewodę w celu monitorowania realizacji świadczeń wychowawczych oraz w celu umożliwienia organom właściwym i wojewodom weryfikacji prawa do świadczeń wychowawczych oraz przez podmioty wymienione w ust. 4 w celu, w jakim informacje te zostały im udostępnione. Organy właściwe i wojewodowie przekazują dane do rejestru centralnego, wykorzystując systemy teleinformatyczne, o których mowa w ust. 1. Informacje zawarte w rejestrze centralnym, o którym mowa w ust. 2, udostępnia się, w zakresie niezbędnym do realizacji ich zadań ustawowych, następującym podmiotom: (1) organowi właściwemu i wojewodzie – w celu weryfikacji danych dotyczących osób ubiegających się o przyznanie świadczenia wychowawczego, osób

spełnienia wielu wymogów RODO, w tym m.in. dot. celowości przetwarzania danych, adekwatności, przejrzystości i precyzyjności, proporcjonalności zakresu gromadzonych danych do celu przetwarzania, konieczności tworzenia centralnego rejestru, procedury udostępniania danych z rejestru i precyzyjności wskazywania podmiotów, którym te dane są udostępnianie, okresów przechowywania, powierzeń, czy bezpieczeństwa przechowywania.

Podsumowanie

System ochrony danych osobowych w Polsce wprowadzony ustawą z 1997 roku, która dokonała implementacji dyrektywy 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, był pierwszym specjalnie dedykowanym reżimem prawnym ochrony prywatności w zakresie przetwarzania danych osobowych osób fizycznych, regulowanym na poziomie ustawowym w Polsce. Wcześniej występowały wyłącznie normy sektorowe, materialno-prawnie odnoszące się do przedmiotu poddawanej regulacji. Zawierały one (często wyłącznie „przy okazji") przepisy chroniące jedynie poszczególne kategorie informacji. Normy konstytucyjne i ustawowe weszły w życie niemal w tym samym czasie. Oczywiście nie można zapominać o przepisach międzynarodowych, których Polska była i nadal pozostaje stroną. Wprowadzony reżim przez okres ponad 20-letni nie pozostawał martwy, cały czas ewoluując zarówno na poziomie legislacyjnym (będąc uzupełnianym o kolejne nowelizacje), jak i wykładniczym (wraz z publikowaniem kolejnych komunikatów, interpretacji czy decyzji administracyjnych GIODO, Grupy Roboczej

pobierających świadczenie wychowawcze oraz dzieci, na które osoby te pobierają świadczenie wychowawcze lub ubiegają się o przyznanie świadczenia wychowawczego; 2) organowi właściwemu, o którym mowa w art. 3 pkt 11 ustawy z dnia 28 listopada 2003 r. o świadczeniach rodzinnych, i wojewodzie – w celu weryfikacji danych dotyczących osób ubiegających się o świadczenia rodzinne, osób pobierających świadczenia rodzinne oraz członków ich rodzin; 3) organowi właściwemu dłużnika, o którym mowa w art. 2 pkt 9 ustawy z dnia 7 września 2007 r. o pomocy osobom uprawnionym do alimentów (Dz. U. z 2019 r. poz. 670, 730, 1802 i 1818), i organowi właściwemu wierzyciela, o którym mowa w art. 2 pkt 10 tej ustawy – w celu weryfikacji danych dotyczących osób ubiegających się o świadczenia z funduszu alimentacyjnego, osób pobierających świadczenia z funduszu alimentacyjnego i członków ich rodzin oraz danych dotyczących dłużników alimentacyjnych; 4) jednostkom organizacyjnym pomocy społecznej prowadzonym przez jednostki samorządu terytorialnego – w celu weryfikacji danych dotyczących osób ubiegających się o świadczenia z pomocy społecznej, osób pobierających świadczenia z pomocy społecznej oraz członków ich rodzin. 4a. Minister właściwy do spraw rodziny przetwarza dane w zakresie adresu poczty elektronicznej wskazanego we wniosku o ustalenie prawa do świadczenia wychowawczego w celu przekazywania informacji związanych z uprawnieniami dla rodzin. Minister właściwy do spraw rodziny przechowuje informacje w rejestrze centralnym, o którym mowa w ust. 2, przez okres 10 lat od dnia zaprzestania udzielania świadczenia wychowawczego, z wyjątkiem informacji dotyczących osób, którym świadczenie nie zostało przyznane, które przechowuje się przez okres 1 roku od dnia, w którym decyzja w sprawie świadczenia stała się ostateczna, lub od dnia pozostawienia wniosku o ustalenie prawa do świadczenia bez rozpatrzenia. 6. Podmioty wymienione w ust. 4 przechowują informacje, o których mowa w ust. 2, przez okres 10 lat od dnia ich udostępnienia z rejestru centralnego, o którym mowa w ust. 2, z wyjątkiem informacji dotyczących osób, którym świadczenie wychowawcze nie zostało przyznane, które przechowuje się przez okres 1 roku od dnia, w którym decyzja w sprawie świadczenia stała się ostateczna, lub od dnia pozostawienia wniosku o ustalenie prawa do świadczenia bez rozpatrzenia. 7. Informacje, o których mowa w ust. 2, usuwa się niezwłocznie po upływie okresów przechowywania, o których mowa w ust. 5 i 6. 8. Minister właściwy do spraw rodziny udostępnia ministrowi właściwemu do spraw finansów publicznych, na jego żądanie, dane, o których mowa w ust. 2, w celu niezbędnym do wykonywania zadań analitycznych. Minister właściwy do spraw finansów publicznych dokonuje pseudonimizacji udostępnionych danych. Art. 14a. 1. Bank krajowy oraz spółdzielcza kasa oszczędnościowo-kredytowa, o których mowa w art. 13 ust. 5 pkt 3, oraz Zakład Ubezpieczeń Społecznych, na potrzeby złożenia wniosku i załączników do wniosku określonych w art. 13 ust. 4, składanych w postaci elektronicznej za pomocą systemu, o którym mowa odpowiednio w art. 13 ust. 5 pkt 2 lub 3, w imieniu organu właściwego, przetwarzają następujące dane osobowe dotyczące osób ubiegających się o świadczenie wychowawcze oraz członków ich rodzin: (1) imię i nazwisko; (2) datę urodzenia; (3) adres miejsca zamieszkania; (4) stan cywilny; 5) obywatelstwo; (6) płeć; (7) numer PESEL, a w przypadku gdy nie nadano numeru PESEL – numer i serię dokumentu potwierdzającego tożsamość; (8) adres poczty elektronicznej i numer telefonu – w przypadku osoby występującej o przyznanie świadczenia wychowawczego – o ile je posiada; (9) dochód; (10) informacje wynikające z zaświadczeń i oświadczeń, o których mowa w art. 13 ust. 4 pkt 3. Zob. art. 14 oraz 14a ustawy z dnia 11 lutego 2016 r. o pomocy państwa w wychowywaniu dzieci (t.j. Dz. U. z 2019 r. poz. 2407). Organy administracji publicznej realizują ustawę przy pomocy systemów teleinformatycznych stanowiących integralne części systemów teleinformatycznych stosowanych do realizacji świadczeń rodzinnych określonych w ustawie z dnia 28 listopada 2003 r. o świadczeniach rodzinnych (Dz. U. z 2018 r. poz. 2220, z późn. zm.1). Zob. art. 14 ustawy z dnia 11 lutego 2016 r. o pomocy państwa w wychowywaniu dzieci (t.j. Dz. U. z 2019 r. poz. 2407; z 2021 r. poz. 1162).

art. 29, jak również z uprawomocnianiem się kolejnych orzeczeń sądów administracyjnych i cywilnych), w tym również samej praktyki podmiotów pracujących na tych przepisach (np. tworzących i wdrażających systemy ochrony danych osobowych u poszczególnych administratorów danych). W rozdziale wskazano jedynie wybrane przykłady zmian prawnych – arbitralnie wyselekcjonowanych z perspektywy ich doniosłości dla porządku prawnego.

Należy mieć na uwadze, że ochrona danych osobowych jest specyficzną domeną prawa albowiem obejmuje dziedzinę życia społeczno-ekonomicznego, która ulega bardzo dynamicznym przemianom. Stąd ten specyficzny reżim jest wręcz modelowym przykładem dziedziny prawa, która jedynie stara się nadążyć za szybko zmieniającym się otoczeniem. Analiza zmian prawnych w systemie ochrony danych osobowych, jako wycinka szerszej kategorii informacji fluktuujących we współczesnym porządku społecznym, niewątpliwie przyczynia się do zrozumienia współzależności pomiędzy prawem a dorobkiem cywilizacyjnym społeczeństw, gdzie informacja przesyłana w czasie rzeczywistym przekracza granice polityczne nie dbając o porządki prawne przestrzeni, na którą oddziałuje.

Ustawa z 1997 była nowelizowana wielokrotnie. Aby potwierdzić tezę, iż system ochrony danych osobowych (jako odrębna gałąź prawna) stanowi proces posłużono się wybranymi przykładami jego ewolucji. Egzemplifikacją stała się kwestia definicji danych osobowych (jako zagadnienia fundamentalnego dla samej istoty ochrony), udostępnienie danych osobowych, oraz (w ramach pakietu deregulacyjnego) poluzowanie obostrzeń w zakresie rejestracji zbiorów danych osobowych i zmiany zasad przekazywania danych do państw trzecich.

I tak polska ustawa z 1997 roku w pierwotnym brzmieniu za dane osobowe uznawała każdą informację dotyczącą osoby fizycznej, pozwalającą na określenie tożsamości tej osoby (cechą wyróżniającą dane osobowe od innych informacji dotyczących osób jest tzw. brak anonimowości). Dane osobowe nabywały swój status w momencie, w którym dało się ustalić tożsamość jednostki, której dane dotyczą. Taka redakcja przepisu rodziła skutek w postaci tego, że przedmiotem ochrony ustawy nie były wszystkie dane o osobach fizycznych lecz jedynie tzw. dane identyfikujące. Tymczasem, zgodnie z utrwalonym stanowiskiem, informacją o charakterze osobowym jest nie tylko taka informacja, która dotyczy konkretnej osoby (fr. *identifiée*), ale również taka, której tożsamość można ustalić (fr. *identifiable* – dosłownie identyfikowalna) na podstawie innych udostępnionych danych. Dopiero nowelizacje ustawy dokonane w 2001 roku oraz w 2004 roku wyprostowały tę lukę prawną.

Udostępnianie danych osobowych od samego początku obowiązywania ustawy z 1997 roku, stanowiło przedmiot kontrowersji i sporów prawnych. Przepis, który początkowo powstał na potrzeby administratorów sektora publicznego, od 2004 roku objął również podmioty spoza sfery prawa publicznego, co rodziło niekończące się dylematy w zakresie stosowania normy. Tym bardziej, że ustawa utrzymała w mocy art. 51 ustawy, który z kolei stypizował

sankcję karną za udostępnienie danych, przez podmiot administrujący zbiorem danych lub podmiot zobowiązany do ochrony danych osobowych, osobom nieupoważnionym. Narosły węzeł gordyjski przecięła dopiero nowelizacja z 2011 roku uchylająca przepis art. 29 ustawy.

Wreszcie w ramach pakietu deregulacyjnego 1 stycznia 2015 roku weszły w życie znowelizowane przepisy:

a) w zakresie obowiązku rejestracji zbiorów danych oraz powoływania Administratorów Bezpieczeństwa Informacji (powołanie ABI i zgłoszenie go GIODO do rejestracji umożliwiało przesunięcie obowiązku prowadzenia rejestru zbiorów danych w jednostce organizacyjnej z GIODO na ABI i likwidację obowiązku zgłoszenia zbioru do rejestracji GIODO na podstawie art. 43 ust. 1 ustawy, przy czym obowiązkowi rejestracji nadal podlegały zbiory, jeżeli były w nich przetwarzane dane wrażliwe).
b) dopuszczając możliwość przekazywania danych osobowych do państw trzecich bez potrzeby uzyskania na to zgody wyrażonej przez Generalnego Inspektora Ochrony Danych Osobowych.

Na tle charakteru zmian należy uznać, iż kolejne nowelizacje dobitnie unaoczniały swoistą rywalizację wartości, z jednej strony ochrony prywatności, bezpieczeństwa danych osób fizycznych (jako elementu międzynarodowej i konstytucyjnej ochrony praw człowieka), z drugiej realizację celów publicznych, lub za nie uważanych, które uzasadniały zawężanie owej prywatności w wybranych dziedzinach funkcjonowania sektora publicznego. Ta dwoistość ujawniała się najczęściej w równoległym zabieganiu sektora prywatnego oraz wybranych organów publicznych (Rzecznika Prawa Obywatelskich, Generalnego Inspektora Ochrony Danych Osobowych) o przestrzeganie zasad ochrony danych osobowych oraz nadwyrężania tego systemu przez normodawcę, który próbował wielokrotnie bądź to wyłączać przedmiotowo lub podmiotowo konieczność stosowania niektórych wymogów wobec podmiotów publicznych, bądź przez legislacyjne osłabianie rygorów.

REFORMA NA GRUNCIE ROZPORZĄDZENIA 2016/679

Struktura systemu ochrony danych osobowych od 25 maja 2018 roku

Motywy wprowadzenia RODO

Punktem odniesienia dla adresatów norm w zakresie ochrony danych osobowych w Polsce, do czasu wejścia w życie reformy europejskiego systemu ochrony danych osobowych, pozostawała polska ustawa o ochronie danych osobowych z 1997 roku, stanowiąca implementacje zasad wprowadzonych dyrektywą 95/46/WE. Podobnie we wszystkich pozostałych państwach unijnych krajowe ustawy stanowiły podstawę prawną systemów ochrony danych osobowych. Stąd też decyzja o przygotowaniu reformy reżimu normatywnego – jako rezultatu oczywistej konieczności dostosowania prawa do nowych wyzwań cywilizacyjnych[87].

Należy mieć na uwadze charakter aktu prawnego, jakim jest dyrektywa, która oddziałuje na krajowe systemy prawne państw członkowskich jedynie pośrednio. Stypizuje ramy minimalnych standardów i celów jakie winien osiągnąć ustawodawca krajowy. Obliguje państwa członkowskie, zgodnie z art. 288 TFUE, do osiągnięcia wskazanych w niej rezultatów, określając wyłącznie minimalny wymagany zakres dostosowania. Jednocześnie umożliwia regulowanie danej dziedziny przez państwo członkowskie w stopniu przekraczającym minimalne wymagania. W konsekwencji dyrektywa, z uwagi na specyficzny charakter konsekwencji prawnych, nie tworzy całkowicie jednolitego porządku prawnego w strefie państw Unii Europejskiej[88]. Stąd każdy kraj członkowski wdraża dyrektywę trochę

[87] Szerzej na temat zmian cywilizacyjnych związanych z epoką informacyjną zob. literatura przedmiotu, w tym m.in.: J.B. Abramson, F.Ch. Artertone, C.R. Orren, *The Electronic Commonwealth: The Impact of New Media Technologies in Democratic Politics*, Nowy Jork 1988; U. Beck, *Władza i przeciwwładza w epoce globalnej: nowa ekonomia polityki światowej*, przeł. J. Łoziński, Warszawa 2005; M. Castells, P. Himanen, *Społeczeństwo informacyjne i państwo dobrobytu*, przeł. M. Penkala, M. Sutowski, Krytyka Polityczna nr 17, Warszawa 2009; M. Castells, *Galaktyka Internetu. Refleksje nad Internetem, biznesem i społeczeństwem*, przeł. T. Hornowski, Poznań 2003; M. Castells, *Koniec tysiąclecia*, przeł. J. Stawiński, S. Szymański, Warszawa 2009; M. Castells, *Społeczeństwo sieci*, przeł. M. Marody, K. Pawluś, J. Stawiński, S. Szymański, Warszawa 2007; M. Castells, *The Informational City: Information technology, Economic Restructuring and Urban Regional Process*, Blackwell, Oxford, Cambridge, MA 1989; D. Dziuba, *Gospodarki nasycone informacją i wiedzą*, Warszawa 2001; A. Florini, *The Third Force: The Rise of Transnational Civil Society*, Nowy Jork 2000;; *Problemy społeczeństwa informacyjnego. Elementy analizy, ewaluacji i prognozy*, red. L. Zacher, Warszawa 1997; R. Robertson, *Globalization: Social Theory and Global Culture*, Londyn 1992; E. Rogers, L. Kincaid, *Communication Networks: Towards a New Paradigm for Research*, Nowy Jork 1981; A.M. Rosie, *Teoria przesyłania informacji*, przeł. J. Zalewski, Warszawa 1978; J. Stiglitz, *Globalizacja*, przeł. H. Simbierowicz, Warszawa 2007; *The Information Age: An Anthology on Its Impact and Consequences*, red. D.S., Alberts, D.S., Papp, CCRP Publication Series, Waszyngton 1997; *The Value and Impact of Information*, red. M., Feeneay, M., Grieves, East Grinstead, West Sussex 1994; A. Toffler, *Budowa nowej cywilizacji. Polityka trzeciej fali*, przeł. J. Łoziński, Poznań 1996; A. Toffler, *Trzecia fala*, przeł. E. Wojdyłło, Warszawa 1986; A. Touraine, *Critique de la modernite*, Fayard, Paryż 1992; A. Touraine, *Myśleć inaczej*, przeł. M. Byliniak, Warszawa 2011; A. Touraine, *Un nouveau paradigme*, Fayard, Paryż 2005; I. Wallerstein, *Koniec świata jaki znamy*, przeł. M. Bilewicz, A.W. Jelonek, K. Tyszka, Warszawa 2004; B.H. Zisk, *The Politics of Transformation: Local Activism in the Peace and Environmental Movements*, Westport 1992.

[88] K. Zalewska-Wojtuś, *Dyrektywa jako źródło prawa*, Energia Elektryczna 2010, nr 2.

„po swojemu". Podobnie rzecz się miała w przypadku dyrektywy 95/46/WE. Poszczególne państwa członkowskie *de facto* miały własne systemy ochrony danych osobowych. W obliczu wyzwań cywilizacyjnych określających współczesny, ponadgraniczny, globalny charakter przetwarzania informacji, taki model stawał się coraz bardziej przestarzały i dysfunkcjonalny[89].

Pomiędzy wejściem w życie dotychczasowej dyrektywy 95/46/WE w 1995 roku a rozporządzeniem 2016/679 (RODO) w maju 2018 roku upłynęły 23 lata, co z perspektywy zmian w obszarze przesyłania i gromadzenia informacji, w tym danych osobowych, stanowiło „wieki świetlne". Można zaryzykować stwierdzenie, że w tym czasie dokonała się kolejna rewolucja informacyjna a społeczeństwa przeszły od czasów analogowych do cyfrowych, wraz nowymi oczekiwaniami i zagrożeniami (zarówno jakościowymi, jak i ilościowymi). Interdyscyplinarna analiza relacji na linii społeczeństwa – informacja pozwala ujawnić kanały przepływu informacji w przestrzeni publicznej[90]. Istnieje dostatecznie dużo przesłanek uzasadniających supozycję o występowaniu zjawiska władztwa informacyjnego, którego podstawą jest potencjał tkwiący w informacji, po pierwsze – jako źródła wiedzy o zdarzeniach i procesach, po drugie – źródła ocen wizerunkowych, po trzecie – źródła nadawania znaczeń określonym faktom, po czwarte – podstawy kształtowania określonych zachowań politycznych. Władztwo informacyjne nie ma jednego źródła pochodzenia, centralnego ośrodka, endogennego rdzenia. Jest hybrydą wszystkiego, współtworząc inteligentny, szybko uczący się i dostosowujący system (*smart system*). System korelacyjny, ekspansywny, inkluzywny, chłonny, symultaniczny, wreszcie niewyczerpywalny[91]. System metainformacyjny, postnowoczesny i eksploatujący wszystkie zasoby. Jednocześnie wraz z nowymi zjawiskami zwiększa się pula różnorodności zagrożeń dla szeroko rozumianego bezpieczeństwa, wymagających nowych form odpowiedzi i strategii[92].

Wraz z nowymi uwarunkowaniami nastąpiło odejście od klasycznie rozumianych form zinstytucjonalizowanego rządzenia na rzecz wielozależnościowych struktur cywilizacyjnych. Zdigitalizowani obywatele są w stanie dysponować większą siłą wpływu na ostateczny scenariusz cywilizacyjny niż ośrodki władzy. Jednocześnie dokonało się przekształcenie dotychczasowej przestrzeni społecznej w elektroniczną przestrzeń sieciową, a w konsekwencji przejście od *representative democracy* do *information democracy*[93]. Prawa sfery informacyjnej i technologicznej (opisywane przez informatykę, cybernetykę) zostały

[89] Należy mieć jednak na uwadze, że w przestrzeni Wspólnot kwestie ochrony prywatności jednostki w zderzeniu z postępem technologicznych były wcześniej dostrzegane i poruszane. Zob. m.in. Rezolucja Parlamentu Europejskiego z 21.02.1975 r. w sprawie ochrony praw jednostek w odniesieniu do postępu technicznego w dziedzinie automatycznego przetwarzania danych (Dz.U. WE z 1975 r. Nr C 60, s. 48); Rezolucja Parlamentu Europejskiego z 8.05.1979 r. w sprawie ochrony praw jednostek w odniesieniu do postępu technicznego w dziedzinie automatycznego przetwarzania danych (Dz.U. WE z 1979 r. Nr C 140, s. 34); Komunikat Komisji Europejskiej z 13.09.1990 r. na temat ochrony jednostek w związku z przetwarzaniem danych osobowych we Wspólnocie oraz bezpieczeństwa informacji, COM(90) 314 final, CELEX: 51990DC0314.

[90] Szerzej zob. C. Martysz, *Informacja publiczna czy chronione dane osobowe* [w:] *Ochrona danych osobowych wczoraj, dziś, jutro*, GIODO, Warszawa 2006

[91] Szerzej zob. A. Rogala-Lewicki, *Informacja jako autonomiczny czynnik wpływu w przestrzeni publicznej. Studium władztwa informacyjnego*, Wydawnictwo naukowe Grategia, Częstochowa 2017.

[92] Zob. Wspólny komunikat Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów z 7.02.2013 r. „Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń", JOIN(2013) 1 final.

[93] Szerzej na temat wpływu informacji na procesy demokratyczne zob. A. Rogala-Lewicki, *Relacje informacyjne państwo – obywatel na tle zależności między e-rządem według Matthew Symondsa, fazami rozwoju demokracji Roberta Alana Dahla, a partycypacją obywatelską* [w:] *Cyberpolitologia. Badanie polityki w Internecie*, red. D. Mider, A. Maksymowicz, Warszawa 2013.

zintegrowane z prawami rządzącymi relacjami społecznymi[94]. Relewantna okazała się być siła natężenia zmian w takich przestrzeniach jak:

a) wolumen ilości informacji,
b) szybkość i częstotliwości dokonywania transferów,
c) odległości między sferą władzy a sferą obywatelską,
d) wykorzystywanie różnych metod przekazu,
e) przekształcenie sygnału z analogowego na cyfrowy,
f) powszechność sieci,
g) gromadzenie (metodami jawnymi i niejawnymi) informacji,
h) udostępnianie informacji,
i) wymiana informacji,
j) współzależność (*multidependency*),
k) podejście do zarządzania informacją,
l) otoczenie prawne, w tym ustawodawstwa gwarantujące dostęp do informacji publicznej, możliwości ponownego jej wykorzystania i transparentności (*open state*, *open data*, *open government*, *re-use data*),
m) otoczenie prawne w zakresie metod pozyskiwania informacji kolidujących z normami demokratycznymi,
n) otoczenie prawne w zakresie informatyzowania usług publicznych (np. *e-goverment*, *e-voting*),
o) wielkość środków finansowych przeznaczanych na infrastrukturę informacyjną,
p) edukacja cyfrowa, w tym biegłość informacyjnej (*information literacy*),
q) partycypacja społeczno-obywatelska (*social engagement*)[95],
r) wzajemne podejście podmiotów relacji.

W konsekwencji pojawił się nowy system wartości, nastąpiła zmiana mentalna. Każdy nowy czynnik, zarówno informacyjny, jak i metainformacyjny stał się relewantny dla kondycji społeczeństw. Pod pojęciem nowego paradygmatu społecznego ukrywały nowe formy: struktury wielopoziomowej, wielopodmiotowej i wielopłaszczyznowej. Procesy społeczno-polityczne zaczęły charakteryzować się relacyjnymi układami niewładczymi. Uwolnione zostały podziały na państwo i społeczeństwo, na zwierzchnika i podwładnych[96]. Miejsce poleceń i rozkazów zajęły różnego typu interakcje, w tym m.in. konsultacje, uzgodnienia, negocjacje, pakty. Wszystko wpisane już nie w układ stosunków wewnętrznych, krajowych, lecz porządek

[94] Szerzej zob. D. Brin, *The Transparent Society*, Nowy Jork 2009.
[95] Szerzej na partycypacji obywatelskiej zob. A. Rogala-Lewicki, *Citizens' involvement in public sphere – information as a ius publicum factor of the state of democracy,* European Journal of Geopolitics, Nr 5/2017
[96] Na temat uwolnienia barier pozwalających na bezgraniczną inwigilacje społeczeństw zob. m.in. M. Rojszczak, *Prawne podstawy prowadzenia masowej inwigilacji obywateli opartej na hurtowym i nieukierunkowanym przechwytywaniu danych w UE z uwzględnieniem dorobku orzeczniczego TSUE i ETPC*, Studia Prawa Publicznego 2017, nr 2, s. 159–187. Por. P. Chrzczonowicz, V. Kwiatkowska-Darul, K. Skowroński, *Społeczeństwo inwigilowane w państwie prawa*, wyd. UMK, Toruń 2003.

globalny. Poszerzona przestrzeń dyskursu[97], globalizacja, informatyzacja, technologizacja życia, komputeryzacja, usieciowienie, cyfryzacja, nowe sposoby komunikacji, integracja ponadnarodowa, umiędzynarodowienie kontaktów politycznych i ekonomicznych, mediatyzacja i tabloidyzacja sfery publicznej[98] – to wszystko kategorie bezpośrednio zmieniające charakter współczesnych relacji społecznych[99].

Oprócz wyżej wspomnianych przyczyn o charakterze ogólnocywilizacyjnym pojawiły się także bardziej konkretne, które można uznać za bezpośrednie powody przygotowania i wdrożenia reformy systemu ochrony danych osobowych w UE, w tym m.in.

1) o charakterze ekonomicznym: (a) pojawienie się nowych globalnych podmiotów przetwarzających dane osobowe na masową skalę (np. Apple, Facebook, Google, Yahoo, Youtube, Microsoft, itp.), (b) objęcie kontrolą globalnego kapitału finansującego cyfrowe instrumenty przetwarzania danych, (c) zwiększenie kontroli nad procesami przetwarzania;
2) jak i o charakterze prawnym: (a) nadużywanie prawa przez państwa członkowskie[100], (b) nieprzestrzeganie norm wspólnotowych, bądź nieprawidłowe wdrożenie dyrektywy, (c) potrzeba doprecyzowania praw przysługujących podmiotom, których dane są przetwarzane, (d) wprowadzenie nowych definicji, jak dane genetyczne, czy dane o stanie zdrowia, (e) uwzględnienie przetwarzania danych osobowych w grupach kapitałowych, (f) konieczność uwzględnienia nowego orzecznictwa, np. wyroków Trybunału Sprawiedliwości UE w tzw. sprawach Safe Harbour, jak i Privacy Shield.

Łącznie czynniki te wpłynęły na stan dezaktualizacji dyrektywy 95/46/WE[101].

W wyniku wejścia w życie rozporządzenia 2016/679 (RODO) bezpośrednie, a więc jednolite stosowanie przepisów przez państwa członkowskie, wykluczyło rozbieżności między

[97] Na temat wolności słowa a ochrony prywatności zob. wyrok TK z 30.06.2006, sygn. P 10/06, OTK-A 2006, nr 9, poz. 128.

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

[99] Szerzej zob. literatura przedmiotu, w tym m.in.: M. Foucault, *Filozofia, Historia, Polityka – wybór pism*, Warszawa, Wrocław 2000; T. Goban-Klas, *Cywilizacja medialna. Geneza, ewolucja, eksplozja*, Warszawa 2005; T. Goban-Klas, *Społeczeństwo informacyjne. Szanse, zagrożenia, wyzwania*, Kraków 1999; J. Habermas, *Filozoficzny dyskurs nowoczesności*, przeł. M. Łukaszewicz, Kraków 2000; J. Habermas, *Strukturalne przeobrażenia sfery publicznej*, przeł. W. Lipnik, M. Łukaszewicz, Warszawa 2007; D. Held, *Democracy and the global order: From the modern state to Cosmopolitan Governance*, Stanford 1995; D. Held, A. McGrew, D. Goldblatt, J. Perraton, *Global Transformations: Politics, Economics and Culture*, Stanford 1999; A. Mattelart, *Społeczeństwo informacji*, przeł. J. Mikułowski, Kraków 2004; M. Mazur, *Jakościowa teoria informacji*, Warszawa 1970; M. McLuhan, *Zrozumieć media. Przedłużenie człowieka*, przeł. N. Szucka, Warszawa 2004.

[100] Należy mieć na uwadze, że społeczne funkcjonowanie w zdigitalizowanym świecie co rusz uderza w konstytucyjne gwarancje ochrony prywatności, w tym w tajemnicę komunikowania się głównie jako rezultat dynamicznego rozwoju Internetu, w tym portali społecznościowych. Wyraźnie zarysowuje się tendencja do pozyskiwania, przechowywania i przesyłania zgromadzonych informacji w postaci elektronicznej. Wśród tych informacji znaczną część stanowią dane osobowe, które zgodnie z obowiązującymi regulacjami powinny być szczególnie chronione. Taki model komunikacji utrudnia zachowanie gwarancji prawnych stworzonych w interesie każdego obywatela do obrony przed nieuprawnionym naruszeniem szeroko rozumianej sfery prywatności. Tymczasem poufność jest jednym z elementów szerszej prawa (wartości), jaką jest godność człowieka, naturalnym prawem do dysponowania informacjami osobistymi. Szerzej zob. R.A. Dahl, B. Stinebrickner, *Współczesna analiza polityczna*, przeł. P.M. Kazimierczak, Scholar, Warszawa 2010; X. Dai, *Digital Revolution and Governance*, Ashgate Publication, Londyn 2000; *Decydowanie publiczne*, red. G. Rydlewski, Warszawa 2011; K. Krzysztofek, *Władza i obywatel w społeczeństwie informacyjnym*, Warszawa 1999; L. Porębski, *Elektroniczne oblicze polityki – demokracja, państwo, instytucje polityczne w okresie rewolucji informacyjnej*, Kraków 2004; *Public sector information in the Digit al Age. Between Markets, Public Management and Citizens' Rights*, red. G. Aichholzer, H. Burkert, Cheltenham UK, Northhampton Masachusetts USA, 2004; A. Rothert, *Cybernetyczny porządek polityczny*, Warszawa 2005; A. Rothert, *Technopolis, wirtualne sieci polityczne*, Warszawa 2003; G. Rydlewski, *Rządzenie w świecie megazmian*, Warszawa 2009; J. Scott, *Władza*, przeł. S. Królak, Warszawa 2006; *Sfera publiczna. Kondycja, przejawy, przemiany*, red. J.P., Hudzik, W., Woźniak, Lublin 2006; E. Wnuk-Lipiński, *Świat miedzyepoki. Globalizacja. Demokracja. Państwo narodowe*, Kraków 2004.

[101] Zob. Rezolucja Parlamentu Europejskiego z dnia 6.07.2011 r. w sprawie całościowego podejścia do kwestii ochrony danych osobowych w Unii Europejskiej, P7_TA(2011)0323 (CELEX: 52011IP0323, Dz. Urz. UE z 2013r. Nr CE 33, s. 101). Por. Komunikat Komisji Europejskiej z 4.11.2010 do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów: „Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej", COM(2010) 609.

zakresami ochrony danych w ramach Unii[102]. Należy jednak mieć na uwadze, iż pomimo ujednolicenia zasad ochrony danych, wykonawcze przepisy krajowe, oraz te pozostające poza domeną Wspólnoty, a regulujące ich przetwarzanie w zakresie nieobjętym rozporządzeniem, w poszczególnych państwach członkowskich nadal się nieznacznie różnią – co jednak mieści się w kompetencjach państw członkowskich wynikających z traktatów lub innych unijnych aktów prawa pochodnego o randze równej rozporządzeniu[103].

RODO w części wskazującej na uwarunkowania relewantne dla przyjęcia aktu prawnego podaje aż 173 tzw. motywy, wyróżniając szereg różnych czynników. Jak wskazują komentatorzy Maciej Kawecki i Tomasz Osiej „w przypadku tak wielu nowych rozwiązań motywy zawarte w preambule nabierają wyjątkowego znaczenia. Mają ułatwić ich interpretację, a tym samym sprawić, że dostosowywanie się do nowych przepisów będzie mogło przebiegać w tym samym kierunku. Warto również podkreślić, że z motywów nie będą korzystać tylko administratorzy, inspektorzy ochrony danych czy Trybunał, ale i EROD, która będzie mogła wydawać wytyczne co do tego, jak wdrożyć odpowiednie środki oraz wykazać przestrzeganie prawa przez administratora lub podmiot przetwarzający dane – w szczególności, jeżeli chodzi o identyfikowanie ryzyka związanego z przetwarzaniem, o jego ocenę pod kątem źródła, charakteru, prawdopodobieństwa i wagi zagrożenia oraz o najlepsze praktyki pozwalające zminimalizować to ryzyko (motyw 77 preambuły RODO). Ponadto motywy będą pomocne przy tworzeniu kodeksów postępowań, certyfikacji lub sugestiach inspektora ochrony danych"[104]. Poniżej przeglądowo wybrane motywy RODO jak następuje:

- ochrona osób fizycznych w związku z przetwarzaniem danych osobowych jest jednym z praw podstawowych a przepisy dot. przetwarzania danych osobowych nie mogą naruszać podstawowych praw i wolności;
- przetwarzanie danych osobowych należy zorganizować w taki sposób, aby służyło ludzkości; prawo do ochrony danych osobowych nie jest prawem bezwzględnym; należy je przestrzegać w kontekście jego funkcji społecznej i wyważyć względem innych praw podstawowych w myśl zasady proporcjonalności;
- integracja społeczno-gospodarcza wynikająca z funkcjonowania rynku wewnętrznego doprowadziła do zwiększenia transgranicznych przepływów danych; szybki postęp techniczny i globalizacja przyniosły nowe wyzwania w dziedzinie ochrony danych osobowych;
- cele i zasady dyrektywy 95/46/WE pozostają aktualne, jednak wdrażając ochronę danych w Unii, nie uniknięto fragmentaryzacji, niepewności prawnej oraz upowszechnienia poglądu, że ochrona jest znacznie zagrożona, w szczególności w związku z działaniami w Internecie;

[102] Szerzej zob. Komunikat Komisji do PE i Rady Wzmocniona ochrona, nowe możliwości – wytyczne Komisji dotyczące bezpośredniego stosowania ogólnego rozporządzenia o ochronie danych od dnia 25 maja 2018 r., Bruksela, 24.1.2018r. COM(2018) 43 final.
[103] Szerzej zob. Komunikat Komisji do PE i Rady Ochrona danych jako filar wzmacniania pozycji obywateli oraz podejścia UE do transformacji cyfrowej – dwa lata stosowania ogólnego rozporządzenia o ochronie danych [SWD(2020) 115 final], Bruksela, 24.6.2020 r. COM(2020) 264 final.
[104] *Ogólne rozporządzenie o ochronie danych osobowych. Wybrane zagadnienia,* red. M. Kawecki, T. Osiej, wyd. C.H. Beck, Warszawa 2017.

- aby zapewnić spójny stopień ochrony osób fizycznych należy zagwarantować pewność prawa i przejrzystość, ten sam poziom prawnie egzekwowalnych praw oraz obowiązków oraz neutralność techniczną;
- aby osoby fizyczne nie zostały pozbawione ochrony, przetwarzanie danych osobowych osób, których dane dotyczą, znajdujących się w Unii, powinno podlegać rozporządzeniu, jeżeli czynności przetwarzania wiążą się z oferowaniem takim osobom towarów lub usług, niezależnie od tego czy pociąga to za sobą płatność;
- przetwarzanie danych osobowych znajdujących się w Unii osób, których dane dotyczą, przez administratora lub podmiot przetwarzający, którzy nie mają jednostki organizacyjnej w Unii, powinno podlegać rozporządzeniu;
- zasady ochrony danych powinny mieć zastosowanie do wszelkich informacji o zidentyfikowanych lub możliwych do zidentyfikowania osobach fizycznych;
- „spseudonimizowane" dane osobowe, które przy użyciu dodatkowych informacji można przypisać osobie fizycznej, należy uznać za informacje o możliwej do zidentyfikowania osobie fizycznej;
- „pseudonimizacja" danych osobowych może ograniczyć ryzyko dla osób, których dane dotyczą, oraz pomóc administratorom i podmiotom przetwarzającym wywiązać się z obowiązku ochrony danych;
- dane genetyczne należy zdefiniować jako dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, uzyskane z analizy próbki biologicznej danej osoby fizycznej, w szczególności z analizy chromosomów, kwasu dezoksyrybonukleinowego (DNA) lub kwasu rybonukleinowego (RNA) lub z analizy innych elementów umożliwiających pozyskanie równoważnych informacji;
- do danych osobowych dotyczących zdrowia należy zaliczyć wszystkie dane o stanie zdrowia osoby, której dane dotyczą, ujawniające informacje o przeszłym, obecnym lub przyszłym stanie fizycznego lub psychicznego zdrowia osoby, której dane dotyczą, przy czym do danych takich należą informacje o danej osobie fizycznej zbierane podczas jej rejestracji do usług opieki zdrowotnej lub podczas świadczenia jej usług opieki zdrowotnej, jak to określa dyrektywa Parlamentu Europejskiego i Rady 2011/24/UE numer, symbol lub oznaczenie przypisane danej osobie fizycznej w celu jednoznacznego zidentyfikowania tej osoby fizycznej do celów zdrowotnych, informacje pochodzące z badań laboratoryjnych lub lekarskich części ciała lub płynów ustrojowych, w tym danych genetycznych i próbek biologicznych; oraz wszelkie informacje, na przykład o chorobie, niepełnosprawności, ryzyku choroby, historii medycznej, leczeniu klinicznym lub stanie fizjologicznym lub biomedycznym osoby, której dane dotyczą, niezależnie od ich źródła, którym może być na przykład lekarz lub inny pracownik służby zdrowia, szpital, urządzenie medyczne lub badanie diagnostyczne in vitro;

- główną jednostką organizacyjną administratora w Unii powinno być miejsce, w którym znajduje się jego centralna administracja w Unii, chyba że decyzje co do celów i sposobów przetwarzania danych osobowych zapadają w innej jednostce organizacyjnej administratora w Unii;
- grupa przedsiębiorstw powinna obejmować przedsiębiorstwo sprawujące kontrolę oraz przedsiębiorstwa kontrolowane, przy czym przedsiębiorstwo sprawujące kontrolę powinno być przedsiębiorstwem, które może wywierać dominujący wpływ na pozostałe przedsiębiorstwa ze względu na przykład na strukturę właścicielską, udział finansowy lub przepisy regulujące jego działalność, lub też uprawnienia do nakazywania wdrożenia przepisów o ochronie danych osobowych, przy czym za grupę przedsiębiorstw należy uznać przedsiębiorstwo kontrolujące przetwarzanie danych osobowych w przedsiębiorstwach powiązanych z nim, wraz z tymi przedsiębiorstwami;
- 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;
- wszelkie przetwarzanie danych osobowych powinno być zgodne z prawem i rzetelne, przy czym 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 a 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;
- aby przetwarzanie danych było zgodne z prawem, powinno się odbywać na podstawie zgody osoby, której dane dotyczą, lub na innej uzasadnionej podstawie przewidzianej prawem, przy czym 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, natomiast zgody nie uważa się za dobrowolną, jeżeli nie można jej wyrazić z osobna na różne operacje przetwarzania danych osobowych;
- przetwarzanie danych osobowych do celów innych niż cele, w których dane te zostały pierwotnie zebrane, powinno być dozwolone wyłącznie w przypadkach, gdy jest zgodne z celami, w których dane osobowe zostały pierwotnie zebrane;
- każda osoba fizyczna powinna mieć prawo dostępu do zebranych danych jej dotyczących oraz powinna mieć możliwość łatwego wykonywania tego prawa w rozsądnych odstępach czasu, by mieć świadomość przetwarzania i móc zweryfikować zgodność przetwarzania z prawem;

- każda osoba fizyczna powinna mieć prawo do sprostowania danych osobowych jej dotyczących oraz prawo do „bycia zapomnianym", jeżeli zatrzymywanie takich danych narusza prawo, przy czym prawo to ma znaczenie w przypadkach, gdy osoba, której dane dotyczą, wyraziła zgodę jako dziecko, gdy nie była w pełni świadoma ryzyka związanego z przetwarzaniem, a w późniejszym czasie chce usunąć takie dane osobowe, w szczególności z Internetu;
- osoba, której dane dotyczą, powinna mieć prawo do tego, by nie podlegać decyzji – mogącej obejmować określone środki – która ocenia jej czynniki osobowe, opiera się wyłącznie na przetwarzaniu zautomatyzowanym i wywołuje wobec osoby, której dane dotyczą, skutki prawne lub w podobny sposób znacząco na nią wpływa, jak na przykład automatyczne odrzucenie elektronicznego wniosku kredytowego czy elektroniczne metody rekrutacji bez interwencji ludzkiej, przy czym 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 – o ile wywołuje skutki prawne względem tej osoby lub w podobny sposób znacząco na nią wpływa;
- 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; lub jeżeli przetwarzane są dane osobowe osób wymagających szczególnej opieki, w szczególności dzieci; jeżeli

przetwarzanie dotyczy dużej ilości danych osobowych i wpływa na dużą liczbę osób, których dane dotyczą, przy czym prawdopodobieństwo i powagę ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, należy określić poprzez odniesienie się do charakteru, zakresu, kontekstu i celów przetwarzania danych, a ryzyko należy oszacować na podstawie obiektywnej oceny, w ramach której stwierdza się, czy z operacjami przetwarzania danych wiąże się ryzyko lub wysokie ryzyko;

- dla zachowania zgodności z niniejszym rozporządzeniem, administrator lub podmiot przetwarzający powinni prowadzić rejestry czynności przetwarzania, za które są odpowiedzialni, a każdy administrator i każdy podmiot przetwarzający powinni mieć obowiązek współpracować z organem nadzorczym i na jego żądanie udostępniać mu te rejestry w celu monitorowania tych operacji przetwarzania;
- w celu zachowania bezpieczeństwa i zapobiegania przetwarzaniu niezgodnemu z niniejszym rozporządzeniem administrator lub podmiot przetwarzający powinni oszacować ryzyko właściwe dla przetwarzania oraz wdrożyć środki – takie jak szyfrowanie – minimalizujące to ryzyko, natomiast aby poprawić przestrzeganie 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;
- administrator powinien przed przetwarzaniem dokonać oceny skutków dla ochrony danych, aby ocenić konkretne prawdopodobieństwo i powagę tego wysokiego ryzyka, uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz źródła ryzyka;
- po stwierdzeniu naruszenia ochrony danych osobowych administrator powinien zgłosić je organowi nadzorczemu bez zbędnej zwłoki, jeżeli to wykonalne, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia, chyba że administrator jest w stanie wykazać zgodnie z zasadą rozliczalności, że jest mało prawdopodobne, by naruszenie to mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych.
- przepływ danych osobowych do państw spoza Unii i do organizacji międzynarodowych oraz z takich państw i z takich organizacji jest niezbędnym warunkiem rozwoju handlu międzynarodowego i współpracy międzynarodowej;
- aby zapewnić spójne monitorowanie i egzekwowanie rozporządzenia w całej Unii, organy nadzorcze powinny mieć w każdym państwie członkowskim te same zadania i faktyczne uprawnienia, w tym uprawnienia do prowadzenia postępowań wyjaśniających, naprawcze, uprawnienia do nakładania kar oraz do udzielania zezwoleń i doradcze, w szczególności w przypadku skarg osób fizycznych;
- każda osoba, której dane dotyczą, powinna mieć prawo wniesienia skargi do jednego organu nadzorczego oraz prawo do skutecznego środka ochrony prawnej przed sądem, zgodnie z art. 47 Karty praw podstawowych;

- w celu wzmocnienia i zharmonizowania sankcji administracyjnych za naruszenie rozporządzenia każdy organ nadzorczy powinien być uprawniony do nakładania administracyjnych kar pieniężnych, przy czym w akcie prawnym należy wymienić rodzaje naruszeń oraz wskazać górną granicę i kryteria ustalania związanych z nimi administracyjnych kar pieniężnych, które właściwy organ nadzorczy powinien określać indywidualnie dla każdego przypadku z uwzględnieniem wszystkich stosownych okoliczności danej sytuacji, z należytym uwzględnieniem w szczególności charakteru, wagi, czasu trwania naruszenia i jego konsekwencji, a także środków podjętych w celu zastosowania się do obowiązków wynikających z rozporządzenia oraz w celu zapobieżenia konsekwencjom naruszenia lub w celu zminimalizowania tych konsekwencji;
- w sytuacjach, w których rozporządzenie nie harmonizuje sankcji administracyjnych, lub w razie potrzeby w innych przypadkach, na przykład w razie poważnego naruszenia rozporządzenia, państwa członkowskie powinny wdrożyć system przewidujący skuteczne, proporcjonalne i odstraszające sankcje;
- prawo państw członkowskich powinno godzić przepisy regulujące wolność wypowiedzi i informacji, w tym wypowiedzi dziennikarskiej, akademickiej, artystycznej lub literackiej, z prawem do ochrony danych osobowych na mocy rozporządzenia, przy czym przetwarzanie danych osobowych jedynie do celów dziennikarskich lub do celów wypowiedzi akademickiej, artystycznej lub literackiej powinno podlegać wyjątkom lub odstępstwom od niektórych przepisów rozporządzenia, jeżeli jest to niezbędne, by pogodzić prawo do ochrony danych osobowych z prawem do wolności wypowiedzi i informacji, przewidzianymi w art. 11 Karty praw podstawowych.

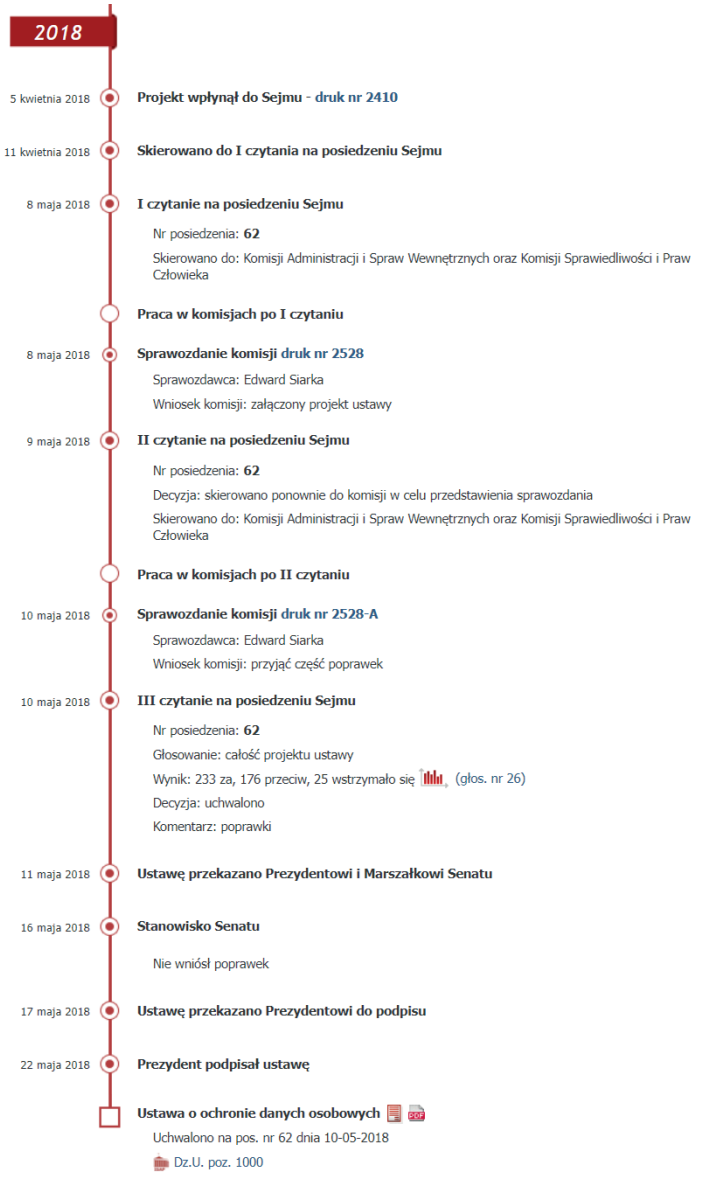
Podsumowując można zaryzykować konstatację, iż unijna reforma systemu ochrony danych osobowych, stanowi próbę dostosowania reżimu prawnego do dokonującego się postępu cywilizacyjnego (w szczególności technologicznego i społecznego). Przy tym trzeba mieć na uwadze fakt, że ujęcie prawne materii tak niezwykle dynamicznej jest i zawsze będzie stanowić cykl – proces bez ostatecznego kształtu.

Ewolucja treści nowej ustawy o ochronie danych osobowych

W Polsce nowy system ochrony danych osobowych – obok RODO – współtworzą ustawa z 10 maja 2018 r. o ochronie danych osobowych, (2) ustawa z dnia 9 maja 2018 r. o przetwarzaniu danych dotyczących przelotu pasażera, (3) ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, (4) ustawa z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania 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). Ostateczny kształt polskiej ustawy o ochronie danych osobowych był kompromisem wynikającym z wieloletnich prac nad kolejnymi wersjami projektu ustawy.

RYSUNEK 1 Droga legislacyjna ustawy o ochronie danych osobowych



Źródło: Rządowy projekt ustawy o ochronie danych osobowych, druk 2410, https://www.sejm.gov.pl/sejm8.nsf/PrzebiegProc.xsp?nr=2410, [dostęp: 12.12.2020]

Chociaż projekt, który został finalnie przyjęty pod obrady i z sukcesem zakończył ścieżkę legislacyjną, był opatrzony jako druk 2410, to jednak należy mieć na uwadze, że nie była to pierwsza wersja ustawy, która już wcześniej przeszła swoją ewaluację na etapie przygotowań i uzgodnień międzyresortowych (jako projekt rządowy)[105].

RYSUNEK 2 Droga międzyresortowa ustawy o ochronie danych osobowych

Źródło: Projekt ustawy o ochronie danych osobowych, https://legislacja.rcl.gov.pl/projekt/12302950, [dostęp: 12.12.2020]

Konsultacje społeczne projektu trwały od 14 września 2017 roku do 13 października 2017 roku W ich toku opinie do ustawy zgłosiło łącznie ponad 110 organizacji i obywateli, przedstawiając ponad 700 stron uwag. Należy odnotować co najmniej trzy główne warianty projektów

[105] Szerzej na temat projektu ustawy o ochronie danych osobowych zob. Projekt ustawy o ochronie danych osobowych skierowany na Komitet do Spraw Europejskich Rady Ministrów, Serwis Rzeczypospolitej Polskiej gov.pl, https://www.gov.pl/cyfryzacja/projekt-ustawy-o-ochronie-danych-osobowych-skierowany-na-komitet-do-spraw-europejskich-rady-ministrow, [dostęp: 02.12.2020].

nowej ustawy o ochronie danych osobowych [(1) z 28 marca 2017 roku[106], (2) z 12 września 2017 roku[107], (3) z 8 lutego 2018 roku[108])], kształt finalny aktu z 10 maja 2018 roku, który wszedł w życie 25 maja 2018 roku oraz wersję po dwóch nowelizacjach z 1 października 2018 roku[109] oraz 4 maja 2019 roku[110], przy czym 30 sierpnia 2019 roku ogłoszono tekst jednolity ustawy[111].

Projekt ustawy z 28 marca 2017 roku należy traktować jako dość wstępną wersję aktu. Wystarczy porównać jego objętość czy ilość tytułów (rozdziałów), czy zakres materialnoprawny z kolejnym projektem z 12 września 2017 roku. I tak, na tak prozaicznym poziomie, pierwszy liczy 17 stron, 8 rozdziałów i 61 przepisów, podczas gdy drugi liczy 30 stron, 11 rozdziałów i 92 przepisy. Do projektu ustawy, na przestrzeni kilku miesięcy, włączono korekty niektórych postanowień[112] oraz trzy nowe rozdziały dot.: Prezesa Urzędu Ochrony Danych Osobowych[113], odpowiedzialności karnej[114] oraz przepisów końcowych[115]. Co ważne, w dokumencie z 12 września 2017 roku, wskazano po raz pierwszy pierwotną wersję bezpośrednich adresatów norm, tj. organy publiczne wskazane w art. 5 § 2 pkt 3 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego oraz podmioty publiczne wskazane w art. 9 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych, ograniczenia w stosowaniu ustawy[116], rozstrzygnięcia oraz zakres materialny aktu. Projekt wskazywał, że ustawa określa:

1) podmioty obowiązane do wyznaczenia inspektora ochrony danych oraz tryb zawiadamiania o wyznaczaniu;
2) warunki i tryb udzielania certyfikacji i akredytacji

[106] Projekt ustawy o ochronie danych osobowych z dnia 28 marca 2017 roku, https://www.gov.pl/web/cyfryzacja/projekt-ustawy-o-ochronie-danych-osobowych, [dostęp: 05.12.2021].

[107] Projekt ustawy o ochronie danych osobowych z 12 września 2017 r., https://odoserwis.pl/a/1149/projekt-ustawy-o-ochronie-danych-osobowych-z-dnia-12-wrzesnia-2017-r, [dostęp: 05.12.2021].

[108] Projekt ustawy o ochronie danych osobowych skierowany na Komitet do Spraw Europejskich Rady Ministrów, https://www.gov.pl/web/cyfryzacja/projekt-ustawy-o-ochronie-danych-osobowych-skierowany-na-komitet-do-spraw-europejskich-rady-ministrow, [dostęp: 02.12.2021].

[109] Ustawa z dnia 3 lipca 2018 r. – Przepisy wprowadzające ustawę – Prawo o szkolnictwie wyższym i nauce (Dz.U. 2018 poz. 1669).

[110] Ustawa z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania 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), Dz.U. z 2019 r. poz. 730.

[111] Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 30 sierpnia 2019 r. w sprawie ogłoszenia jednolitego tekstu ustawy o ochronie danych osobowych (t.j. Dz.U. z 2019 r. poz. 1781).

[112] Przykładowo usunięto postanowienia dotyczące opracowywania i udostępniania na stronie internetowej przez Prezesa UODO dobrych praktyk przetwarzania danych osobowych, uszczegółowiono moment podjęcia czynności kontrolnych, utworzono Fundusz Ochrony Danych Osobowych, czy doprecyzowano przepisy regulujące katalog rozstrzygnięć Prezesa w drodze decyzji (w tym kwestię uchylania zaskarżonej decyzji i wydania nowej). Zob. Projekt ustawy o ochronie danych osobowych z 12 września 2017 r., https://odoserwis.pl/a/1149/projekt-ustawy-o-ochronie-danych-osobowych-z-dnia-12-wrzesnia-2017-r, [dostęp: 05.12.2021].

[113] W rozdziale zatytułowanym „Prezes Urzędu Ochrony Danych Osobowych" wprowadzono postanowienia dotyczące: sposobu powoływania, odwoływania, doboru kandydatów, kompetencji, kadencji, liczby zastępców, immunitetu, pociągnięcia do odpowiedzialności, wymogu publikacyjnego na BIP, czy działania Rady do Spraw Ochrony Danych Osobowych. Przykładowo ustalono, że PUODO m.in.: (1) zatwierdza wiążące reguły korporacyjne, o których mowa w art. 47 rozporządzenia, (2) zatwierdza kodeks postępowania, o którym mowa w art. 40 rozporządzenia, (3) przyjmuje standardowe klauzule ochrony danych, o których mowa w art. 46 ust. 2 lit d rozporządzenia, (4) udziela zezwolenia, o którym mowa w art. 46 ust. 3 rozporządzenia. Zob. Rozdział 4 Projektu ustawy o ochronie danych osobowych z 12 września 2017 r., https://odoserwis.pl/a/1149/projekt-ustawy-o-ochronie-danych-osobowych-z-dnia-12-wrzesnia-2017-r, [dostęp: 05.12.2021].

[114] Art. 89.1. Kto udaremnia lub utrudnia kontrolującemu prowadzenie kontroli przestrzegania przepisów o ochronie danych osobowych, podlega grzywnie. 2. Orzekanie w sprawach o czyny określone w ust. 1 następuje w trybie przepisów ustawy z dnia 24 sierpnia 2001 r. – Kodeks postępowania w sprawach o wykroczenia. Art. 90.1. Kto bez podstawy prawnej przetwarza dane, o których mowa w art. 9 rozporządzenia 2016/679, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku. 2. Orzekanie w sprawach o czyny, o których mowa w ust.1, następuje w trybie przepisów ustawy z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego. Zob. art. 89 i 90 Projektu ustawy o ochronie danych osobowych z 12 września 2017 r., https://odoserwis.pl/a/1149/projekt-ustawy-o-ochronie-danych-osobowych-z-dnia-12-wrzesnia-2017-r, [dostęp: 05.12.2021].

[115] W przepisach końcowych przewidziano ówcześnie maksymalny limit wydatków z budżetu państwa przeznaczonych na wykonywanie zadań wynikających z ustawy, który miał wynosić w roku: (1) 2018 r. – 27 214 000 zł., (2) 2019 r. – 16 298 000 zł., (3) 2020 r. – 16 509 000 zł., (4) 2021 r. – 16 285 000 zł., (5) 2022 r. – 16 515,000 zł., (6) 2023 r. – 16 285,000 zł., (7) 2024 r. – 16 516,000 zł., (8) 2025 r. – 16 285 000 zł., (9) 2026 r. – 16 515 000 zł., (10) 2027 r. – 18 015 000 zł. Art. 91 Projektu ustawy o ochronie danych osobowych z 12 września 2017 r., https://odoserwis.pl/a/1149/projekt-ustawy-o-ochronie-danych-osobowych-z-dnia-12-wrzesnia-2017-r, [dostęp: 05.12.2021].

[116] Do działalności polegającej na redagowaniu, przygotowaniu, tworzeniu lub publikowaniu materiałów prasowych w rozumieniu ustawy z dnia 26 stycznia 1984 r. – Prawo prasowe a także do działalności literackiej lub artystycznej nie stosuje się przepisów art. 5–9, 11, 13–16, 18–22, 27, 28 ust. 2–10 i art. 30 rozporządzenia 2016/679. Do wypowiedzi akademickiej o której mowa w art. 85 ust. 2 rozporządzenia 2016/679 nie stosuje się przepisów art. 13, 15 ust. 3u i 4, art. 18, 27, 28 ust. 2–10 i art. 30 rozporządzenia 2016/679. Zob. art. 2 Projektu ustawy o ochronie danych osobowych z 12 września 2017 r., https://odoserwis.pl/a/1149/projekt-ustawy-o-ochronie-danych-osobowych-z-dnia-12-wrzesnia-2017-r, [dostęp: 05.12.2021].

3) organ właściwy w sprawie ochrony danych osobowych;
4) postępowanie w sprawie naruszenia przepisów o ochronie danych osobowych;
5) europejską współpracę administracyjną;
6) postępowanie kontrolne;
7) odpowiedzialność cywilną za naruszenie przepisów o ochronie danych osobowych;
8) administracyjne kary pieniężne za naruszenie przepisów o ochronie danych osobowych.

Z kolei najistotniejsze zmiany w projekcie ustawy z dnia 8 lutego 2018 roku w stosunku do projektu z dnia 12 września 2017 roku prezentuje zestawienie jak w tabeli poniżej.

TABELA 4 Ewolucja treści ustawy o ochronie danych osobowych (porównanie projektów z 12 września 2017 r. i 8 lutego 2018 r.)

ZESTAWIENIE NAJWAŻNIEJSZYCH ZMIAN W PROJEKCIE USTAWY Z DNIA 8 LUTEGO 2018 r. W STOSUNKU DO PROJEKTU Z DNIA 12 WRZEŚNIA 2017 r.			
Lp.	**Projekt z 12 września 2017 r.**	**Projekt z 8 lutego 2018 r.**	**Zwięzła charakterystyka zmian**
1.	Brak analogicznego przepisu	Art. 3. 1. Do przetwarzania danych osobowych przez administratorów nie będących podmiotami publicznymi wskazanymi w art. 9 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2017 r. poz. 2077), zatrudniających mniej niż 250 osób, przepisów art. 13 ust. 2 lit a-b oraz d – f, art. 15 ust. 3 i 4, art. 19 oraz art. 34 rozporządzenia 2016/679 nie stosuje się	Zmiana polegała na znacznym ograniczeniu obowiązku informacyjnego w przypadku zbierania danych od osoby. Przedsiębiorcy zatrudniający poniżej 250 osób nie musieli informować m.in. o: profilowaniu, okresie retencji oraz podawać informacji o większości praw przysługujących osobie. Ponadto osoba nie miała prawa do uzyskania kopii danych, jak również administrator nie musiał jej zawiadamiać o naruszeniu ochrony danych
2.	Art. 4 Przez organy i podmioty publiczne obowiązane do wyznaczenia inspektora, o których mowa w art. 37 ust. 1 lit. a rozporządzenia 2016/679, rozumie się organy publiczne wskazane w art. 5 § 2 pkt 3 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego oraz podmioty publiczne wskazane w art. 9 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych	Art. 7. Przez organy i podmioty publiczne obowiązane do wyznaczenia inspektora ochrony danych, zwanego dalej „inspektorem", o których mowa w art. 37 ust. 1 lit. a rozporządzenia 2016/679, rozumie się organy oraz podmioty publiczne wskazane w art. 9 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych	Zmiana polegała na ograniczeniu organów i podmiotów publicznych zobowiązanych do wyznaczenia IOD. Ograniczenie to dotyczyło: ministrów, centralnych organów administracji rządowej, wojewodów, działających w ich lub we własnym imieniu innych terenowych organów administracji rządowej (zespolonej i niezespolonej), organów jednostek samorządu terytorialnego oraz organów i podmiotów wymienionych w art. 1 pkt 2 KPA, tj. gdy są one powołane z mocy prawa lub na podstawie porozumień do załatwiania spraw indywidualnych rozstrzyganych w drodze decyzji administracyjnych albo załatwianych milcząco
3.	Art. 6. Certyfikacji, o której mowa w art. 42 rozporządzenia 2016/679, dokonuje Prezes Urzędu	Art. 12. Certyfikacji, o której mowa w art. 42 rozporządzenia 2016/679, dokonuje Prezes Urzędu i podmioty akredytowane przez Polskie Centrum Akredytacji, zwane dalej „podmiotami certyfikującymi	Rozszerzenie podmiotów mogących udzielać certyfikacji na przedsiębiorców akredytowanych przez Polskie Centrum Akredytacji. Dotychczas certyfikaty mógł wystawiać jedynie organ
4.	Art. 8. Certyfikacji dokonuje się na wniosek administratora lub podmiotu przetwarzającego	Art. 14. 1. Certyfikacji dokonuje się na wniosek administratora, podmiotu przetwarzającego, producenta albo podmiotu wprowadzającego produkt na rynek	Rozszerzono zakres jednostek uprawnionych do wystąpienia o certyfikację. W poprzednim projekcie z wnioskiem mogli wystąpić jedynie administrator i podmiot przetwarzający. W nowszym projekcie również producent oraz podmiot wprowadzający produkt na rynek

5.	Art. 20 ust. 4 Na stanowisko Prezesa Urzędu może być powołana osoba, która spełnia następujące warunki: 1) jest obywatelem polskim; 2) posiada tytuł naukowy doktora; 3) posiada wiedzę z zakresu ochrony danych osobowych; 4) przez okres co najmniej pięciu lat wykonywała czynności bezpośrednio związane z ochroną danych osobowych; 5) korzysta z pełni praw publicznych; 6) nie była skazana prawomocnym wyrokiem za umyślne przestępstwo lub umyślne przestępstwo skarbowe	Art. 29 ust. 4. Na stanowisko Prezesa Urzędu może być powołana osoba, która: 1) jest obywatelem polskim; 2) posiada wyższe wykształcenie; 3) wyróżnia się wiedzą prawniczą i doświadczeniem z zakresu ochrony danych osobowych; 4) przez okres co najmniej pięciu lat wykonywała czynności bezpośrednio związane z ochroną danych osobowych; 5) korzysta z pełni praw publicznych; 6) nie była skazana prawomocnym wyrokiem za umyślne przestępstwo lub umyślne przestępstwo skarbowe; 7) posiada nieskazitelny charakter	W nowym projekcie zmieniono wymagania dotyczące wymogów Prezesa Urzędu. Najważniejszy z nich to zniesienie posiadania tytułu doktora na rzecz wykształcenia wyższego. Ponadto dodano przepis o „nieskazitelnym charakterze" oraz lekko zmodyfikowano brzmienie punkt 3) dotyczącego wiedzy z zakresu ochrony danych
6.	Brak analogicznego postanowienia	Art. 145. Generalny Inspektor Ochrony Danych Osobowych staje się Prezesem Urzędu Ochrony Danych Osobowych i pełni swoją funkcję do czasu upływu kadencji na którą został powołany	Zmiana polegała na utrzymaniu obecnego GIODO do momentu wygaśnięcia jego pierwotnej kadencji jako Prezesa w rozumieniu nowej ustawy zamiast wyboru nowego Prezesa
7.	Art. 45. Gdy prawa osoby przysługujące na mocy przepisów o ochronie danych osobowych zostały naruszone, organizacja społeczna może występować z żądaniem: 1) wszczęcia postępowania, 2) dopuszczenia jej do udziału w postępowaniu, jeżeli jest to uzasadnione celami statutowymi tej organizacji i gdy przemawia za tym interes osoby, której prawa zostały naruszone	Art. 55. W sprawach związanych z ochroną danych osobowych pełnomocnikiem może być przedstawiciel organizacji, do której zadań statutowych należą sprawy związane z ochroną danych osobowych	Wzmocnienie prawa organizacji do udziału w postępowaniu, które nie jest już warunkowane „interesem osoby"
8.	Art. 89.1. Kto udaremnia lub utrudnia kontrolującemu prowadzenie kontroli przestrzegania przepisów o ochronie danych osobowych, podlega grzywnie. 2. Orzekanie w sprawach o czyny określone w ust. 1 następuje w trybie przepisów ustawy z dnia 24 sierpnia 2001 r. – Kodeks postępowania w sprawach o wykroczenia. Art. 90.1. Kto bez podstawy prawnej przetwarza dane, o których mowa w art. 9 rozporządzenia 2016/679, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku. 2. Orzekanie w sprawach o czyny, o których mowa w ust.1, następuje w trybie przepisów ustawy z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (Dz. U. z 2016 r. poz. 1749 z późn. zm.6)	Art. 101. 1. Kto przetwarza dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do których przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch. 2. Jeżeli czyn określony w ust. 1 dotyczy danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, danych genetycznych, biometrycznych, o stanie zdrowia, seksualności lub orientacji seksualnej, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat trzech. Art. 102. Kto udaremnia lub utrudnia kontrolującemu prowadzenie kontroli przestrzegania przepisów o ochronie danych osobowych, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch	Znaczne rozszerzenie przepisów karnych. W poprzednim projekcie kara pozbawienia wolności do 1 roku groziła jedynie za przetwarzanie szczególnych kategorii danych bez podstawy prawnej. W nowym projekcie objęto przepisami karnymi zarówno przetwarzanie danych zwykłych (do 2 lat), jak i znacznie zwiększono karę za przetwarzanie danych wrażliwych (z 1 do 3 lat). Ponadto ustanowiono karę pozbawienia wolności do lat 2 za utrudnianie wykonywania kontroli Prezesowi Urzędu. Ponadto w odniesieniu do kary za przetwarzanie danych wrażliwych zmniejszono precyzyjność przepisu, który w poprzedniej wersji był dużo bardziej dookreślony. Tu jest mowa o przetwarzaniu niedopuszczalnym lub takim, do którego nie jest się uprawnionym a nie o braku podstawy

Źródło: Omówienie projektu ustawy o ochronie danych osobowych, GDPR.pl, https://gdpr.pl/omowienie-projektu-ustawy-o-ochronie-danych-osobowych, [dostęp: 02.12.2021]

Zmiany pomiędzy wersją projektu ustawy o ochronie danych osobowych z 8 lutego 2018 roku a samą treścią ustawy w wariancie ostatecznym objęły liczne modyfikacje. Poza zmianami redakcyjnymi, doprecyzowaniem postanowień dot. obowiązkowego wyznaczania IOD[117], warunków i trybu dokonywania certyfikacji, o której mowa w art. 42 RODO oraz opracowywaniem i zatwierdzaniem kodeksów postępowania oraz warunków i trybu akredytacji podmiotu monitorującego jego przestrzeganie usunięto m.in.:

- art. 5 Projektu, który stanowił, iż w przypadku usług świadczonych drogą elektroniczną oferowanych bezpośrednio osobie, która nie ukończyła lat trzynastu i która przebywa na terytorium Rzeczpospolitej Polskiej, gdy podstawą przetwarzania danych osobowych jest zgoda tej osoby, przetwarzanie danych osobowych możliwe jest wyłącznie po uzyskaniu uprzedniej zgody jej przedstawiciela ustawowego albo po niezwłocznym potwierdzeniu przez przedstawiciela ustawowego zgody wyrażonej przez taką osobę – co oznaczało podniesienie progu uznawalności za dziecko z 13 lat do 16 (i w konsekwencji

[117] Zob. M. Sakowska-Baryła, *Obowiązek wyznaczenia IOD w podmiotach publicznych*, ABI Expert 2017, nr 2.

konieczności uzyskania zgody opiekuna prawnego) w przypadku usług świadczonych drogą elektroniczną oferowanych bezpośrednio osobie, która przebywa na terytorium RP;
- wymóg dla kandydatów na Prezesa UODO wykonywania przez okres co najmniej pięciu lat czynności bezpośrednio związanych z ochroną danych osobowych oraz posiadania nieskazitelnego charakteru;
- postanowienie, zgodnie z którym Prezes Urzędu może zostać odwołany przed upływem kadencji, w przypadku, gdy złożył niezgodne z prawdą oświadczenie lustracyjne, stwierdzone prawomocnym orzeczeniem sądu;
- obowiązek Prezesa UODO zatwierdzania w drodze decyzji standardowych klauzul ochrony danych, o których mowa w art. 46 ust. 2 lit d rozporządzenia;
- obowiązek Prezesa UODO prowadzenia wewnętrznej ewidencji zawiadomień o powołaniach i odwołaniach Inspektorów Ochrony Danych;
- wymóg dokonywania akredytacji zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności;
- podmioty akredytowane przez Polskie Centrum Akredytacji z kręgu podmiotów dokonujących certyfikacji, o której mowa w art. 42 rozporządzenia (przy czym równolegle usunięto tryb wnioskowy administratora, podmiotu przetwarzającego, producenta albo podmiotu wprowadzającego produkt na rynek);
- art. 98. Projektu, który tworzył Fundusz Ochrony Danych Osobowych, którego dysponentem miał być Prezes Urzędu[118].

Jednocześnie w całym akcie prawnym przywołano cel jego wprowadzenia[119], jak również dokonano generalnej transformacji adresatów bezpośrednich ustawy z „organów lub podmiotów publicznych, o których mowa w art. 9 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych" na „jednostki sektora finansów publicznych, instytuty badawcze oraz Narodowy Bank Polski". To te podmioty zostały zobowiązane do wdrożenia RODO w oparciu o polskie przepisy „wykonawcze", tj. ustawę z 2018 roku[120]. Do ostatecznej wersji ustawy, na tle projektu z 8 lutego 2018 roku, dodano m.in. postanowienia jak w tabeli poniżej.

[118] Przepis brzmiał następująco: Fundusz jest państwowym funduszem celowym. Przychodami Funduszu są środki finansowe pochodzące z 1% kar pieniężnych nakładanych przez Prezesa Urzędu. Środku z Funduszu nie mogą być podstawą osiągania przychodu przez pracowników Urzędu. Środki Funduszu przeznacza się na: (1) inicjowanie i podejmowanie przez Prezesa Urzędu przedsięwzięć w zakresie upowszechniania w społeczeństwie wiedzy o potrzebie ochrony danych osobowych oraz ryzyku, przepisach, zabezpieczeniach i prawach związanych z ich przetwarzaniem. Szczególną uwagę poświęca się działaniom skierowanym do dzieci, (2) inicjowanie i podejmowanie przez Prezesa Urzędu przedsięwzięć w zakresie upowszechniania wśród administratorów i podmiotów przetwarzających wiedzy o obowiązkach spoczywających na nich na mocy przepisów o ochronie danych osobowych. Art. 98 Projektu ustawy o ochronie danych osobowych skierowany na Komitet do Spraw Europejskich Rady Ministrów, https://www.gov.pl/web/cyfryzacja/projekt-ustawy-o-ochronie-danych-osobowych-skierowany-na-komitet-do-spraw-europejskich-rady-ministrow, [dostęp: 02.12.2021].

[119] Ustawa służy stosowaniu 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). Ustawa w zakresie swojej regulacji wdraża dyrektywę 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 uchylającą decyzję ramową Rady 2008/977/WSiSW

[120] Zob. T. Banyś, *Wdrażanie nowych elementów systemu ochrony danych osobowych przez podmioty publiczne* [w:] *Polska i europejska reforma ochrony danych osobowych*, red. E. Bielak-Jomaa, D. Lubasz, wyd. Wolters Kluwer, Warszawa 2016, s. 53–62. Por. K. Czajkowska-Matosiuk, *RODO dla samorządu i administracji. Wzory dokumentów z objaśnieniami*, INFOR PL S.A, Warszawa 2018. Por. P. Kowalik, B. Nowakowski, *Zastosowanie ustawy o ochronie danych osobowych w jednostkach sektora publicznego* [w:] A. Gałach, S. Hoc, A. Jedruszczak, K. Kędzierska, P. Kowalik, M. Kuźma, R. Marek, B. Nowakowski, *Ochrona danych osobowych i informacje niejawne w sektorze publicznym*, Wydanie 2, Wydawnictwo C.H. Beck, Warszawa 2015.

TABELA 5 Uzupełnienia ustawy ODO z 10 maja 2018 na tle projektu z 8 lutego 2018

L.p.	Wersja z 10.05.2018r.	Wersja z 8.02.2018r.	Komentarz
1.	Przez organy i podmioty publiczne obowiązane do wyznaczenia inspektora ochrony danych, zwanego dalej „inspektorem", o których mowa w art. 37 ust. 1 lit. a rozporządzenia 2016/679, rozumie się organy oraz podmioty publiczne wskazane w art. 9 ustawy z dnia 27 sierpnia 2009 r. o finansach: 1) jednostki sektora finansów publicznych; 2) instytuty badawcze; 3) Narodowy Bank Polski.	Przez organy i podmioty publiczne obowiązane do wyznaczenia inspektora ochrony danych, zwanego dalej „inspektorem", o których mowa w art. 37 ust. 1 lit. a rozporządzenia 2016/679, rozumie się organy oraz podmioty publiczne wskazane w art. 9 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych	Doprecyzowano adresatów bezpośrednich ustawy
2.	Administrator wykonujący zadanie publiczne nie przekazuje informacji, o których mowa w art. 13 ust. 3 rozporządzenia 2016/679, jeżeli zmiana celu przetwarzania służy realizacji zadania publicznego i niewykonanie obowiązku, o którym mowa w art. 13 ust. 3 rozporządzenia 2016/679, jest niezbędne dla realizacji celów, o których mowa w art. 23 ust. 1 tego rozporządzenia, oraz przekazanie tych informacji: 1) uniemożliwi lub znacząco utrudni prawidłowe wykonanie zadania publicznego, a interes lub podstawowe prawa lub wolności osoby, której dane dotyczą, nie są nadrzędne w stosunku do interesu wynikającego z realizacji tego zadania publicznego lub 2) naruszy ochronę informacji niejawnych. 2. Administrator jest obowiązany poinformować osobę, której dane dotyczą, na jej wniosek, bez zbędnej zwłoki, nie później jednak niż w terminie miesiąca od dnia otrzymania wniosku, o podstawie nieprzekazania informacji, o których mowa w art. 13 ust. 3 rozporządzenia 2016/679	Brak przepisu w finalnej, zaproponowanej treści	Wyłączenie obowiązku informacyjnego, o którym mowa w art. 13 ust. 1–2, wobec administratora wykonującego zadanie publiczne jeżeli planuje on dalej przetwarzać dane osobowe w celu innym niż cel, w którym dane osobowe zostały zebrane
3.	W zakresie nieuregulowanym w art. 14 ust. 5 rozporządzenia 2016/679 administrator wykonujący zadanie publiczne nie przekazuje informacji, o których mowa w art. 14 ust. 1, 2 i 4 rozporządzenia 2016/679, jeżeli służy to realizacji zadania publicznego i niewykonanie obowiązku, o którym mowa w art. 14 ust. 1, 2 i 4 rozporządzenia 2016/679, jest niezbędne dla realizacji celów, o których mowa w art. 23 ust. 1 tego rozporządzenia, oraz przekazanie tych informacji: 1) uniemożliwi lub znacząco utrudni prawidłowe wykonanie zadania publicznego, a interes lub podstawowe prawa lub wolności osoby, której dane dotyczą, nie są nadrzędne w stosunku do interesu wynikającego z realizacji tego zadania publicznego lub 2) naruszy ochronę informacji niejawnych. 2. W przypadku, o którym mowa w ust. 1, administrator zapewnia odpowiednie środki służące ochronie interesu lub podstawowych praw i wolności osoby, której dane dotyczą. 3. Administrator jest obowiązany poinformować osobę, której dane dotyczą, na jej wniosek, bez zbędnej zwłoki, nie później jednak niż w terminie miesiąca od dnia otrzymania wniosku, o podstawie nieprzekazania informacji, o których mowa w art. 14 ust. 1, 2 i 4 rozporządzenia 2016/679	Brak przepisu w finalnej, zaproponowanej treści	Wyłączenie obowiązku informacyjnego, o którym mowa w art. 14 ust. 1–4, wobec administratora wykonującego zadanie publiczne, w przypadku pozyskania danych osobowych od osoby, której dane dotyczą
4.	Administrator wykonujący zadanie publiczne nie przekazuje informacji, o których mowa w art. 15 ust. 1–3 rozporządzenia 2016/679, jeżeli służy to realizacji zadania publicznego i niewykonanie obowiązków, o których mowa w art. 15 ust. 1–3 rozporządzenia 2016/679, jest niezbędne dla realizacji celów, o których mowa w art. 23 ust. 1 tego rozporządzenia, oraz wykonanie tych obowiązków: 1) uniemożliwi lub znacząco utrudni prawidłowe wykonanie zadania publicznego, a interes lub podstawowe prawa lub wolności osoby, której dane dotyczą, nie są nadrzędne w stosunku do interesu wynikającego z realizacji tego zadania publicznego lub 2) naruszy ochronę informacji niejawnych. 2. W przypadku gdy wykonanie obowiązków, o których mowa w art. 15 ust. 1 i 3 rozporządzenia 2016/679, wymaga niewspółmiernie dużego wysiłku związanego z wyszukaniem danych osobowych, administrator wykonujący zadanie publiczne wzywa osobę, której dane dotyczą, do udzielenia informacji pozwalających na wyszukanie tych danych. Przepis art. 64 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego stosuje się odpowiednio. 3. W przypadkach, o których mowa w ust. 1 i 2, administrator zapewnia odpowiednie środki służące ochronie interesu lub podstawowych praw i wolności osoby, której dane dotyczą. 4. Administrator jest obowiązany poinformować osobę, której dane dotyczą, na jej wniosek, bez zbędnej zwłoki, nie później jednak niż w terminie miesiąca od dnia otrzymania wniosku, o podstawie niewykonania obowiązków, o których mowa w art. 15 ust. 1–3 rozporządzenia	Brak przepisu w finalnej, zaproponowanej treści	Wyłączenie obowiązku informacyjnego, o którym mowa w art. 15 ust. 1–3, wobec administratora wykonującego zadanie publiczne, w przypadku wystąpienia sytuacji niezbędności dla realizacji celów, o których mowa w art. 23 ust. 1 tego rozporządzenia

L.p.	Wersja z 10.05.2018r.	Wersja z 8.02.2018r.	Komentarz
5.	Administrator, który otrzymał dane osobowe od podmiotu realizującego zadanie publiczne, nie wykonuje obowiązków, o których mowa w art. 15 ust. 1–3 rozporządzenia, w przypadku gdy podmiot przekazujący dane osobowe wystąpił z żądaniem w tym zakresie ze względu na konieczność prawidłowego wykonania zadania publicznego mającego na celu: 1) zapobieganie przestępczości, wykrywanie lub ściganie czynów zabronionych lub wykonywanie kar, w tym ochronę przed zagrożeniami dla bezpieczeństwa publicznego i zapobieganie takim zagrożeniom; 2) ochronę interesów gospodarczych i finansowych państwa obejmującą w szczególności: a) realizację i dochodzenie dochodów z podatków, opłat, niepodatkowych należności budżetowych oraz innych należności, b) wykonywanie egzekucji administracyjnej należności pieniężnych i niepieniężnych oraz wykonywanie zabezpieczenia należności pieniężnych i niepieniężnych, c) przeciwdziałanie wykorzystywaniu działalności banków i instytucji finansowych do celów mających związek z wyłudzeniami skarbowymi, d) ujawnianie i odzyskiwanie mienia zagrożonego przepadkiem w związku z przestępstwami, e) prowadzenie kontroli, w tym kontroli celno-skarbowych. 2. W przypadku, o którym mowa w ust. 1, administrator udziela odpowiedzi na żądanie wniesione na podstawie art. 15 rozporządzenia 2016/679 w sposób, który uniemożliwia ustalenie, że administrator przetwarza dane osobowe otrzymane od podmiotu wykonującego zadanie publiczne	Brak przepisu w finalnej, zaproponowanej treści	Wyłączenie obowiązku informacyjnego, o którym mowa w art. 15 ust. 1–3, wobec administratora, który otrzymał dane osobowe od podmiotu realizującego zadanie publiczne, w przypadku gdy podmiot przekazujący dane osobowe wystąpił z żądaniem w tym zakresie ze względu na konieczność prawidłowego wykonania zadania publicznego określonego w przepisie
6.	Ustawy oraz rozporządzenia 2016/679 nie stosuje się do: 1) przetwarzania danych osobowych przez administratorów nie będących podmiotami publicznymi wskazanymi w art. 9jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 1, 3, 5, 6 i 14 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych, zatrudniających mniej niż 250 osób, przepisów869 i 1622), w zakresie, w jakim przetwarzanie to jest konieczne do realizacji zadań mających na celu zapewnienie bezpieczeństwa narodowego, jeżeli przepisy szczególne przewidują niezbędne środki ochrony praw i wolności osoby, której dane dotyczą; 2) działalności służb specjalnych w rozumieniu art. 11 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego13 ust. 2 lit a-b oraz Agencji Wywiadu. Art. 6a. 1. Do przetwarzania danych osobowych w ramach wykonywania konstytucyjnych i ustawowych kompetencji Prezydenta Rzeczypospolitej Polskiej, w zakresie nieobjętym bezpieczeństwem narodowym, stosuje się odpowiednio przepisy art. 4–7, art. 11, art. 12, art. 16, art. 17, art. 24 ust. 1 i 2, art. 25 ust. 1 i 2, art. 28–30, art. 32, art. 34, art. 35, art. 37–39 i art. 86 rozporządzenia 2016/679 oraz przepisy art. 6 i art. 11 ustawy. 2. Przetwarzanie danych, o których mowa w art. 9 i art. 10 rozporządzenia 2016/679, następuje w zakresie niezbędnym do realizacji konstytucyjnych i ustawowych kompetencji Prezydenta RP, jeżeli prawa lub wolności osoby, której dane dotyczą, nie są nadrzędne w stosunku do realizacji zadań wynikających z tych kompetencji	Brak przepisu w finalnej, zaproponowanej treści	Wyłączenia podmiotowe stosowania ustawy ODO
7.	Podmiot, który wyznaczył inspektora, może wyznaczyć osobę zastępującą inspektora w czasie jego nieobecności	Brak przepisu w finalnej, zaproponowanej treści	Wprowadzenie możliwości dla podmiotu, który wyznaczył IOD wyznaczenia osoby zastępującej IOD
8.	W sprawach nieuregulowanych w ustawie do postępowań administracyjnych przed Prezesem Urzędu Ochrony Danych Osobowych, zwanym dalej „Prezesem Urzędu", o których mowa w rozdziałach 4–7 i 11, stosuje się ustawę z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego. 2. Postępowanie przed Prezesem Urzędu jest postępowaniem jednoinstancyjnym. 3. Do postanowień wydanych w postępowaniach, o których mowa w ust. 1, na które zgodnie z ustawą z dnia 14 czerwca 1960 r. − Kodeks postępowania administracyjnego służy zażalenie, przepisów o zażaleniu nie stosuje się. 4. Na postanowienia, o których mowa w ust. 3, służy skarga do sądu administracyjnego	W sprawach nieuregulowanych w ustawie do postępowań przed Prezesem Urzędu Ochrony Danych Osobowych, o których mowa w rozdziale 4 i 5, rozdziale 6 z wyłączeniem art. 52, rozdziale 7 i 11 stosuje się przepisy ustawy z dnia 14 czerwca 1960 r − Kodeks postepowania administracyjnego. 2. Postępowanie przed Prezesem Urzędu Ochrony Danych Osobowych jest postępowaniem jednoinstancyjnym	Wprowadzenie skargi do sądu administracyjnego na decyzje PUODO

L.p.	Wersja z 10.05.2018r.	Wersja z 8.02.2018r.	Komentarz
9.	Prezes Urzędu oraz jego zastępcy nie mogą zajmować innego stanowiska, z wyjątkiem stanowiska dydaktycznego, naukowo-dydaktycznego lub naukowego w szkole wyższej, Polskiej Akademii Nauk, instytucie badawczym lub innej jednostce naukowej, ani wykonywać innych zajęć zarobkowych lub niezarobkowych sprzecznych z obowiązkami Prezesa Urzędu. Prezes Urzędu oraz jego zastępcy nie mogą należeć do partii politycznej, związku zawodowego ani prowadzić działalności	Prezes Urzędu nie może zajmować innego stanowiska, z wyjątkiem stanowiska dydaktycznego, naukowo-dydaktycznego lub naukowego w szkole wyższej, Polskiej Akademii Nauk, instytucie badawczym lub innej jednostce naukowej, ani wykonywać innych zajęć zarobkowych lub niezarobkowych sprzecznych z obowiązkami Prezesa Urzędu. Nie mogą należeć do partii politycznej, związku zawodowego ani prowadzić działalności	Objęcie zakazem działalności pozaurzędowej, poza Prezesem UODO, również jego trzech zastępców
10.	Prezes UODO publikuje na własnym BIP: 1) przyjęte standardowe klauzule ochrony danych, o których mowa w art. 46 ust. 2 lit. d rozporządzenia 2016/679; 2) rekomendacje określające środki techniczne i organizacyjne stosowane w celu zapewnienia bezpieczeństwa przetwarzania danych.	Brak przepisu w finalnej, zaproponowanej treści	Poszerzenie obowiązku przedmiotowego Prezesa UODO w zakresie udostępniania na BIP
11.	Prezes Urzędu opracowuje i udostępnia na swojej stronie podmiotowej Biuletynu Informacji Publicznej rekomendacje określające środki techniczne i organizacyjne stosowane w celu zapewnienia bezpieczeństwa przetwarzania danych osobowych. Rekomendacje sporządzane są z uwzględnieniem specyfiki danego rodzaju działalności i podlegają okresowej aktualizacji. Projekt rekomendacji Prezes Urzędu konsultuje z zainteresowanymi podmiotami, których zakresu działania dotyczy dany projekt.	Brak przepisu w finalnej, zaproponowanej treści	Poszerzenie obowiązku przedmiotowego Prezesa UODO w zakresie udostępniania na BIP
12.	1. W celu skonsultowania się z organem nadzorczym administrator danych składa wniosek o przeprowadzenie uprzednich konsultacji, o których mowa w art. 36 ust. 2 RODO. 2. Do wniosku stosuje się odpowiednio przepis art. 63 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego. 3. Jeżeli wniosek nie spełnia wymogów, określonych w art. 36 ust. 3 rozporządzenia 2016/679 oraz art. 63 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego, Prezes Urzędu informuje o nieudzieleniu konsultacji. 4. Organ informuje wnioskodawcę o przyczynach, wskazując przyczyny ich nieudzielenia konsultacji	Brak przepisu w finalnej, zaproponowanej treści	Wprowadzenie wniosku o przeprowadzenie uprzednich konsultacji, o których mowa w art. 36 ust. 2 RODO
13.	Jeżeli w toku postępowania Prezes Urzędu uzna, że istnieją uzasadnione wątpliwości co do zgodności z prawem Unii Europejskiej decyzji Komisji Europejskiej, o której mowa w art. 40 ust. 9 w sprawie kodeksu postępowania, o którym mowa w art. 46 ust. 2 lit. e, oraz decyzji, o której mowa w art. 45 ust. 3 i 5 i art. 46 ust. 2 lit. c rozporządzenia 2016/679, Prezes Urzędu występuje do sądu administracyjnego z wnioskiem o wystąpienie z pytaniem prawnym na podstawie art. 267 Traktatu o funkcjonowaniu Unii Europejskiej w sprawie ważności decyzji Komisji Europejskiej	Jeżeli w toku postępowania Prezes Urzędu uzna, że istnieją uzasadnione wątpliwości co do zgodności z prawem unii europejskiej decyzji Komisji Europejskiej, o której mowa w art. 40 ust. 9, art. 45, art. 46 ust. 2 lit. c rozporządzenia 2016/679, Prezes Urzędu występuje do sądu administracyjnego z wnioskiem o wydanie postanowienia w sprawie ważności decyzji Komisji Europejskiej	Zastąpienie wniosku Prezesa UODO o wydanie postanowienia w sprawie ważności decyzji Komisji Europejskiej wnioskiem Prezesa UODO do sądu administracyjnego o wystąpienie z pytaniem prawnym na podstawie art. 267 Traktatu o funkcjonowaniu Unii Europejskiej w sprawie ważności decyzji Komisji Europejskiej
14.	1. Czynności kontrolnych dokonuje się w obecności kontrolowanego lub osoby przez niego upoważnionej. 2. Kontrolowany jest obowiązany do pisemnego wskazania osoby upoważnionej do reprezentowania go w trakcie kontroli. 3. W razie nieobecności kontrolowanego lub osoby przez niego upoważnionej, upoważnienie do przeprowadzenia kontroli oraz legitymacja służbowa lub inny dokument potwierdzający tożsamość mogą być okazane: 1) innemu pracownikowi kontrolowanego, który może być uznany za osobę, o której mowa w art. osobie czynnej w lokalu przedsiębiorstwa w rozumieniu art. 97 ustawy z dnia 23 kwietnia 1964 r. – Kodeks cywilny lub 2) przywołanemu świadkowi, jeżeli jest funkcjonariuszem publicznym w rozumieniu art. 115 § 13 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny, niebędącemu pracownikiem Urzędu albo osobą, o której mowa w art. 75	W razie nieobecności kontrolowanego lub osoby przez niego upoważnionej, upoważnienie do przeprowadzenia kontroli oraz legitymacja służbowa lub inny dokument potwierdzający tożsamość mogą być okazane: 1) innemu pracownikowi kontrolowanego, który może być uznany za osobę, o której mowa w art. 97 ustawy z dnia 23 kwietnia 1964 r. – Kodeks cywilny), lub 2) przywołanemu świadkowi, jeżeli jest funkcjonariuszem publicznym w rozumieniu art. 115 § 13 ustawy z dnia 6 czerwca 1997 r. − Kodeks karny, oraz nie jest jednocześnie pracownikiem Urzędu albo osobą o której mowa w art. 75	Wprowadzenie obowiązku pisemnego wskazania osoby upoważnionej do reprezentowania podmiotu kontrolowanego podczas kontroli. Doprecyzowanie trybu kontroli podczas nieobecności kontrolowanego
15.	Kontrolę prowadzi się nie dłużej niż 30 dni od dnia okazania kontrolowanemu lub innej osobie wskazanej w przepisach imiennego upoważnienia do przeprowadzenia kontroli oraz legitymacji służbowej lub innego dokumentu potwierdzającego tożsamość. Do terminu nie wlicza się terminów przewidzianych na zgłoszenie zastrzeżeń do protokołu kontroli lub podpisanie i doręczenie protokołu kontroli przez kontrolowanego	Kontrola nie może trwać dłużej niż miesiąc od dnia podjęcia czynności kontrolnych. Do terminu tego nie wlicza się terminów przewidzianych na zgłoszenie zastrzeżeń do protokołu lub podpisanie i doręczenie protokołu przez kontrolowanego	Doprecyzowanie czasu trwania kontroli

L.p.	Wersja z 10.05.2018r.	Wersja z 8.02.2018r.	Komentarz
16.	Ustawa określa: (…) 8) odpowiedzialność cywilną za naruszenie przepisów o ochronie danych osobowych; i postępowanie przed sądem; 9) odpowiedzialność karną i administracyjne kary pieniężne za naruszenie przepisów o ochronie danych	Ustawa określa: (…) 8) odpowiedzialność cywilną za naruszenie przepisów o ochronie danych osobowych; 9) administracyjne kary pieniężne za naruszenie przepisów o ochronie danych osobowych	Uzupełnienie zakresu przedmiotowego ustawy o odpowiedzialność karną i postępowanie przed sądem
17.	W zakresie nieuregulowanym rozporządzeniem 2016/679, do roszczeń z tytułu naruszenia przepisów o ochronie danych osobowych, o których mowa w art. 79 i art. 82 tego rozporządzenia, stosuje się przepisy ustawy z dnia 23 kwietnia 1964 r. – Kodeks cywilny. O wniesieniu pozwu oraz prawomocnym orzeczeniu kończącym postępowanie w sprawie o roszczenie z tytułu naruszenia przepisów o ochronie danych osobowych, o którym mowa w art. 79 lub art. 82 rozporządzenia 2016/679, sąd zawiadamia niezwłocznie Prezesa Urzędu. Prezes Urzędu zawiadomiony o toczącym się postępowaniu niezwłocznie informuje sąd o każdej sprawie dotyczącej tego samego naruszenia przepisów o ochronie danych osobowych, która toczy się przed Prezesem Urzędu lub sądem administracyjnym albo została zakończona. Prezes Urzędu niezwłocznie informuje sąd również o wszczęciu każdego postępowania w sprawie dotyczącej tego samego naruszenia. Sąd zawiesza postępowanie, jeżeli sprawa dotycząca tego samego naruszenia przepisów o ochronie danych osobowych została wszczęta przed Prezesem Urzędu. Sąd umarza postępowanie w zakresie, w jakim prawomocna decyzja Prezesa Urzędu o stwierdzeniu naruszenia przepisów o ochronie danych osobowych lub prawomocny wyrok wydany w wyniku wniesienia skargi, o której mowa w art. 145a § 3 ustawy z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi, uwzględnia roszczenie dochodzone przed sądem. Ustalenia prawomocnej decyzji Prezesa Urzędu o stwierdzeniu naruszenia przepisów o ochronie danych osobowych lub prawomocnego wyroku wydanego w wyniku wniesienia skargi, o której mowa w art. 145a § 3 ustawy z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi, wiążą sąd w postępowaniu o naprawienie szkody wyrządzonej przez naruszenie przepisów o ochronie danych osobowych co do stwierdzenia naruszenia tych przepisów. W sprawach o roszczenia z tytułu naruszenia przepisów o ochronie danych osobowych, które mogą być dochodzone wyłącznie w postępowaniu przed sądem, Prezes Urzędu może wytaczać powództwa na rzecz osoby, której dane dotyczą, za jej zgodą, a także wstępować, za zgodą powoda, do postępowania w każdym jego stadium. W pozostałych sprawach o roszczenia z tytułu naruszenia przepisów o ochronie danych osobowych Prezes Urzędu może wstępować, za zgodą powoda, do postępowania przed sądem w każdym jego stadium, chyba że toczy się przed nim postępowanie dotyczące tego samego naruszenia przepisów o ochronie danych osobowych. W przypadkach, o których mowa w ust. 1 i 2, do Prezesa Urzędu stosuje się odpowiednio przepisy ustawy z dnia 17 listopada 1964 r. – Kodeks postępowania cywilnego o prokuratorze.. Prezes Urzędu, jeżeli uzna, że przemawia za tym interes publiczny, przedstawia sądowi istotny dla sprawy pogląd w sprawach, których przedmiotem jest ochrona sprawie o roszczenie z tytułu naruszenia przepisów o ochronie danych osobowych. Do postępowania w sprawie o roszczenie z tytułu naruszenia przepisów o ochronie danych osobowych, o których mowa w art. 79 i art. 82 rozporządzenia 2016/679, w zakresie nieuregulowanym ustawą stosuje się przepisy ustawy z dnia 17 listopada 1964 r. – Kodeks postępowania cywilnego	Każda osoba, której prawa przysługujące na mocy przepisów o ochronie danych osobowych zostały naruszone cudzym działaniem, może żądać, zaniechania tego działania a także może żądać ażeby ten, kto dopuścił się naruszenia, dopełnił czynności potrzebnych do usunięcia jego skutków. Sąd okręgowy jest właściwy w sprawach roszczeń z tytułu naruszenia przepisów o ochronie danych osobowych, w tym roszczeń z tytułu art. 89 rozporządzenia 2016/679, niezależnie od wartości przedmiotu sporu. Do postępowania w sprawach roszczeń dochodzonych na podstawie art. 89, w zakresie nieuregulowanym ustawą, stosuje się przepisy Kodeksu postępowania cywilnego. W sprawach cywilnych, których przedmiotem jest ochrona danych osobowych, Prezes Urzędu może z urzędu lub na wniosek strony: (1) żądać wszczęcia postępowania, 2) brać udział w toczącym się postępowaniu- na prawach przysługujących prokuratorowi	Doprecyzowanie przepisów dot. odpowiedzialności cywilnej i wprowadzenie przepisów dot. postępowania przed sądem
18.	Na podmioty publiczne, o których mowa w art. 9 pkt 1–12 i 14 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych, 101a. 1. W związku z toczącym się postępowaniem w sprawie nałożenia administracyjnej kary pieniężnej, podmiot, o którym mowa w art. 101, jest obowiązany do dostarczenia Prezesowi Urzędu, na każde jego żądanie, w terminie 30 dni od dnia otrzymania żądania, danych niezbędnych do określenia podstawy wymiaru administracyjnej kary pieniężnej. 2. W przypadku niedostarczenia danych przez podmiot, o którym mowa w art. 101, lub gdy dostarczone przez ten podmiot dane uniemożliwiają ustalenie podstawy wymiaru administracyjnej kary pieniężnej, Prezes Urzędu ustala podstawę wymiaru administracyjnej kary pieniężnej w sposób szacunkowy uwzględniając wielkość podmiotu, specyfikę prowadzonej przez niego działalności lub ogólnie dostępne dane finansowe dotyczące podmiotu	Brak przepisu w finalnej, zaproponowanej treści	Dodanie obowiązków na podmioty w związku z toczącym się postępowaniem w sprawie nałożenia administracyjnej kary pieniężnej
19.	Prezes Urzędu może nałożyć, w drodze decyzji, administracyjne kary pieniężne w wysokości do 10 000 złotych na jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 13 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych	Brak przepisu w finalnej, zaproponowanej treści	Wprowadzenie możliwości karania jednostek kultury

L.p.	Wersja z 10.05.2018r.	Wersja z 8.02.2018r.	Komentarz
20.	1. Kto udaremnia lub utrudnia kontrolującemu prowadzenie kontroli przestrzegania przepisów o ochronie danych osobowych, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch	1. Kto udaremnia lub utrudnia kontrolującemu prowadzenie kontroli przestrzegania przepisów o ochronie danych osobowych, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch. 2. Tej samej karze podlega kto, w związku z toczącym się postępowaniem w sprawie nałożenia administracyjnej kary pieniężnej, nie dostarcza danych niezbędnych do określenia podstawy wymiaru administracyjnej kary pieniężnej lub dostarcza dane, które uniemożliwiają ustalenie podstawy wymiaru administracyjnej kary pieniężnej	Dodanie normy karnej

Źródło: Opracowanie własne na podstawie projektu ustawy o ochronie danych osobowych skierowany na Komitet do Spraw Europejskich Rady Ministrów, https://www.gov.pl/web/cyfryzacja/projekt-ustawy-o-ochronie-danych-osobowych-skierowany-na-komitet-do-spraw-europejskich-rady-ministrow, [dostęp: 02.12.2021] oraz ustawy z 10 maja 2018 o ochronie danych osobowych (Dz.U. 2018 poz. 1000)

Ochrona danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (DODO), dotyczących przelotu pasażera (PNR) oraz o pasażerach (API)

RODO, jako akt prawa powszechnie obowiązującego, jest adresowany abstrakcyjnie, tj. do wszystkich, którzy przetwarzają dane osobowe na terytorium Unii Europejskiej, względnie chcą transferować te dane zagranicę. Niemniej art. 2 ust. 2 rozporządzenia wprowadza przesłankę egzoneracyjną, wyłączającą ściśle określony krąg podmiotów z stosowania (w konkretnych okolicznościach) tego aktu. Przepis stanowi, że rozporządzenie nie ma zastosowania do przetwarzania danych osobowych m.in.: przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom.

Nie oznacza to jednak luki prawnej. Wyżej przywołane organy zostały bowiem zobowiązane do przetwarzania i ochrony danych osobowych na podstawie odrębnego aktu, tj. 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 uchylająca decyzję ramową Rady 2008/977/WSiSW (zwaną „dyrektywą policyjną")[121]. Dyrektywa 2016/680 do polskiego porządku prawnego została implementowana ustawą z dnia 14 grudnia 2018 roku o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości[122] (zwaną też na wzór abrewiacji samego rozporządzenia: ustawą DODO). Należy zatem mieć na uwadze, że od dnia wejścia w życie w/w ustawy, tj. od dnia 6 lutego 2019 roku obowiązuje w Polsce drugi, obok RODO, akt prawny ustalający przesłanki i warunki przetwarzania oraz ochrony danych osobowych[123]. Zarówno RODO, jak i DODO stanowią niezależne

[121] Dz.Urz. UE L 119 z 4.05.2016 s. 89–131.
[122] Dz.U. z 2019 r., poz. 125.
[123] Do 24 maja 2018 roku ochrona danych przetwarzanych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań

od siebie podstawy prawne przetwarzania danych adresowane do innego kręgu podmiotów przetwarzających. Przy czym oba akty się przenikają[124], a podmioty odpowiedzialne za ściganie i zwalczanie przestępczości są zobowiązane również do przestrzegania RODO[125].

RYSUNEK 3 Droga legislacyjna ustawy z dnia 14 grudnia 2018 roku o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości

Źródło: Rządowy projekt ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, druk 2989, https://www.sejm.gov.pl/Sejm8.nsf/PrzebiegProc.xsp?nr=2989, [dostęp: 17.07.2021]

przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar była kompleksowo uregulowana przepisami ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych. Od 25 maja 2018 r. do 5 lutego 2019 r. te kwestie były regulowane utrzymanymi w mocy ustawą z 10 maja 2018 r. o ochronie danych osobowych (Dz.U. poz. 1000 ze zm.) przepisami ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych. Zob. *Ustawa wdrażająca dyrektywę 2016/680, zwana potocznie „policyjną", już obowiązuje*, https://uodo.gov.pl/pl/138/706, [dostęp: 17.07.2021].

[124] Przykładem mogą być definicje wprowadzone przez RODO, które analogicznie stosuje się do DODO jak: administrator danych, dane osobowe, naruszenia ochrony danych osobowych, przetwarzanie danych osobowych. Nadto, oba akty prawne przewidują jeden organ nadzorczy, tj. Prezesa Urzędu Ochrony Danych.

[125] We wszystkich sprawach, w których przetwarzanie danych osobowych odbywa się w jednym z wymienionych celów, mają zastosowanie przepisy wdrażające dyrektywę. Istotnym jest, że podmioty odpowiedzialne za ściganie i zwalczanie przestępczości, przetwarzające dane w celach określonych w przywołanym art. 1 pkt 1 ustawy DODO, zobowiązane są również do stosowania przepisów RODO w pozostałym zakresie, np. rekrutacją pracowników czy prowadzeniem spraw kadrowych. Oznacza to, że mogą pojawić się sytuacje, w których jeden podmiot zobowiązany będzie do spełnienia równolegle wymagań przewidzianych przepisami ustawy DODO oraz RODO. Kluczowa jest znajomość różnic w zakresie obowiązków narzucanych przez oba akty prawne. Szerzej zob. A. Grzelak, *Ustawa o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości. Komentarz*, C.H. Beck, Warszawa 2019.

Zgodnie z art. 1 pkt 1 DODO ustawa określa zasady i warunki ochrony danych osobowych przetwarzanych przez właściwe organy w celu rozpoznawania, zapobiegania, wykrywania i zwalczania czynów zabronionych, w tym zagrożeń dla bezpieczeństwa i porządku publicznego, a także wykonywania tymczasowego aresztowania, kar, kar porządkowych i środków przymusu skutkujących pozbawieniem wolności. Będą to zatem organy związane z szeroko rozumianym zwalczaniem przestępczości, prowadzeniem postępowań karnych, wyrokowaniem i wykonywaniem kar, w odniesieniu do czynności operacyjno-rozpoznawczych, dochodzeniowo-śledczych i administracyjno-porządkowych, przy czym ustawa reguluje nie tylko działalność organów ścigania, lecz również jednostek prokuratury oraz sądów w zakresie objętym ustawą[126]. Nadzór nad przetwarzaniem danych osobowych, których administratorem są sądy i są przetwarzane: (a) w postępowaniach sądowych w ramach sprawowania wymiaru sprawiedliwości albo realizacji zadań z zakresu ochrony prawnej, (b) w ramach sprawowania wymiaru sprawiedliwości albo realizacji zadań z zakresu ochrony prawnej w systemach teleinformatycznych obsługujących postępowania sądowe, oraz w których są prowadzone rejestry sądowe, jak również w których są prowadzone urządzenia ewidencyjne – został powierzony prezesom sądów wyższych instancji i Krajowej Radzie Sądownictwa[127]. Na uwagę także zwraca fakt, iż ustawy nie stosuje się w sprawach danych przetwarzanych przez: Agencję Bezpieczeństwa Wewnętrznego, Agencję Wywiadu, Służbę Kontrwywiadu Wojskowego, Służbę Wywiadu Wojskowego oraz Centralne Biuro Antykorupcyjne – w zakresie zapewnienia bezpieczeństwa narodowego[128].

Podstawowe różnice pomiędzy RODO a DODO można przyporządkować do pięciu najważniejszych kategorii: (1) podstaw prawnych przetwarzania danych osobowych, (2) wymogów posiadania i prowadzenia dokumentacji, (3) prawa osób, których dane dotyczą, (4) obowiązku informacyjnego, oraz (5) konieczności wyznaczenia Inspektora Ochrony Danych, których ilustracją jest tabela jak następuje.

[126] W szczególności należy mieć na uwadze takie organy jak: Sąd Najwyższy, Sądy powszechne, Sądy administracyjne, Sądy wojskowe, Trybunał Konstytucyjny, Trybunał Stanu, Prokuratura, Instytut Pamięci Narodowej, Służba Ochrony Państwa, Policja, Centralne Biuro Śledcze Policji, Straż Graniczna, Straż Miejska, Żandarmeria Wojskowa, Służba Więzienna, Prezes Urzędu Ochrony Konkurencji i Konsumentów, Inspekcja Drogowa, Straż Rybacka, Inspekcja Kontroli Skarbowej, Inspekcja Pracy, Inspekcja Handlowa, Państwowa Inspekcja Sanitarna, Inspekcja Weterynaryjna, Inspekcja Ochrony Środowiska, Państwowa Inspekcja Farmaceutyczna, przewoźnicy lotniczy, podmioty odpowiedzialne za bezpieczeństwo imprez masowych, czy komornik egzekwujący kary zasądzone w postępowaniu karnym. Szerzej zob. S. Serafin, W. Szmulik, *Organy ochrony prawnej RP*, C.H. Beck, Warszawa 2010.

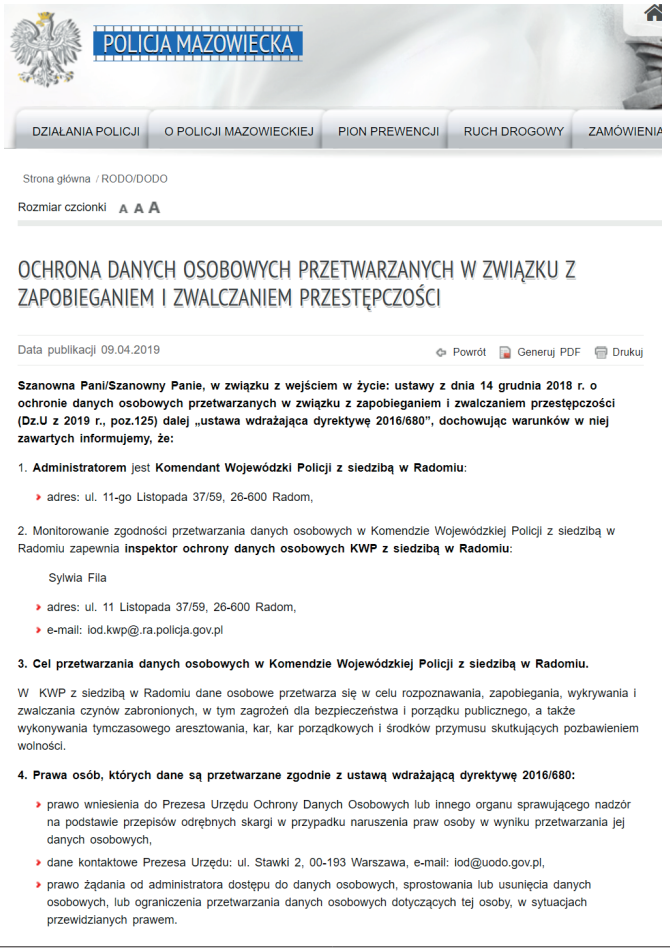
[127] Ustawy z dnia 27 lipca 2001 r. Prawo o ustroju sądów powszechnych reguluje kwestię nadzoru nad przetwarzaniem danych osobowych w sądach. Zgodnie z normą nadzór nad przetwarzaniem danych osobowych, których administratorami są sądy, zgodnie z art. 175da (administratorzy danych osobowych przetwarzanych w systemach teleinformatycznych) i art. 175db (administratorzy danych osobowych przetwarzanych w postępowaniach sądowych), wykonują w zakresie działalności sądu: (1) rejonowego – prezes sądu okręgowego, (2) okręgowego – prezes sądu apelacyjnego, (3) apelacyjnego – Krajowa Rada Sądownictwa. Zob. art. 175dd ustawy z dnia 27 lipca 2001 r. Prawo o ustroju sądów powszechnych (t.j. Dz.U. z 2020 r., poz. 365).

[128] Jak podkreśla się w doktrynie, ustawa – niezgodnie z dyrektywą 2016/680 – wyłącza swoje zastosowanie także do danych osobowych znajdujących się w aktach spraw lub czynności lub urządzeniach ewidencyjnych prowadzonych w postępowaniach: (a) w stosunku do nieletnich, (b) karnych, w tym karnych wykonawczych i karnych skarbowych, (c) wobec osób z zaburzeniami psychicznymi stwarzającymi zagrożenie dla życia, zdrowia lub wolności seksualnej i innych osób. Zob. P. Liwszic, T. Ochocki, Ł. Pociecha, *Ustawa o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości. Komentarz*, C.H. Beck, Warszawa 2019.

TABELA 6 Podstawowe różnice między rozporządzeniem 2016/679 a ustawą o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (implementującą dyrektywę 2016/680)

Lp	RODO	DODO (ustawa)
1.	**Podstawy prawne przetwarzania danych**	
	Podstawy przetwarzania określone a przepisach art. 6–10 RODO (dane zwykłe, dane wrażliwe)	Przetwarzanie danych osobowych na gruncie ustawy DODO możliwe jest tylko i wyłącznie, gdy jest to niezbędne dla realizacji uprawnienia lub spełnienia obowiązków wynikających z przepisów (art. 13 DODO) Dane osobowe szczególnych kategorii mogą być przetwarzane jedynie, gdy przepis prawa zezwala na takie działanie lub jest to niezbędne dla ochrony życia lub zdrowia lub interesów osoby, której dane dotyczą lub innej osoby, bądź też dane tego typu zostały upublicznione przez osobę, której one dotyczą (art. 14 DODO)
2.	**Dokumentacja ochrony danych**	
	W RODO jedynie art. 24 ust. 2 wspomina o właściwym – jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania – wdrożeniu odpowiednich polityk ODO, przy czym przepis nie wprowadza wymogu posiadania fizycznej (papierowej), ale winno to znaleźć odzwierciedlenie w formie zapisu lub opisu (np. w formie elektronicznej). Administratorzy danych są zobowiązani do przyjęcia koncepcji *risk based approach*, w szczególności dokonywania: • rejestru czynności przetwarzania danych (art. 30 ust. 1 RODO) • rejestru kategorii czynności przetwarzania (art. 30 ust. 2 RODO) • raportowania naruszenia bezpieczeństwa danych (art. 33 RODO) • oceny (analizy) ryzyka (art. 24, 32, 35, 36 RODO) • oceny skutków przetwarzania dla danych osobowych (*privacy impact assessment*), (art. 35 RODO)	Zgodnie z art. 31 ust. 4 ustawy DODO, administrator zobowiązany jest do opracowania i wdrożenia polityki ochrony danych osobowych, uwzględniającej sposób dokumentowania zastosowanych przez niego niezbędnych technicznych i organizacyjnych środków, odpowiadającej charakterowi, zakresowi, kontekstowi i celom przetwarzania oraz ryzyku naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia. Za minimalny zakres dokumentacji ochrony danych należy uznać wykaz jak następuje: • obowiązek opracowania i wdrożenia dokumentacji ochrony danych osobowych (art. 31 ust. 4 DODO) • bezwzględny obowiązek prowadzenia wykazu kategorii czynności przetwarzania (art. 35 ust. 1 DODO) • bezwzględny obowiązek prowadzenia wykazu kategorii czynności przetwarzania dokonywanych w imieniu administratora (art. 35 ust. 3 DODO) • obowiązek ewidencjonowania operacji przetwarzania prowadzonych w systemach zautomatyzowanych (art. 36 DODO) • obowiązek prowadzenia ewidencji osób upoważnionych do przetwarzania danych (art. 42 DODO)
3.	**Prawa osób, których dane dotyczą**	
	Prawa osób, których dane dotyczą (art. 15–21 RODO). W stosunku do praw analogicznie przewidzianych w DODO, rozporządzenie zawiera normy regulujące: • prawo do ograniczenia przetwarzania • prawo do przenoszenia danych • prawo do sprzeciwu oraz do niepodleganiu decyzji opartych na zautomatyzowanym przetwarzaniu	• prawo do uzyskania informacji o przetwarzaniu danych osobowych • prawo dostępu do danych oraz uzyskania kopii lub wyciągu z danych • prawo do uzupełnienia, uaktualnienia lub sprostowania danych osobowych • prawo do bycia zapomnianym
4.	**Obowiązek informacyjny**	
	Obowiązek informacyjny (klauzule informacyjne) realizowany w sytuacji, gdy dane osobowe pozyskiwane są bezpośrednio od osoby, której dane dotyczą (art. 13 RODO) oraz pośrednio, bez jej aktywnego działania, np. ze źródeł powszechnie dostępnych (art. 14 RODO)	DODO zawiera przepisy o charakterze *lex specialis* wobec wymogów określonych w art. 13 i 14 RODO. I tak realizacja obowiązku informacyjnego na podstawie *lex generalis*, zgodnie bowiem z art. 22 ustawy DODO, będzie się materializowała w następujących sytuacjach: • publiczne przekazywanie informacji przez administratora danych (art. 22 ust. 1 i ust. 2 DODO) • przekazywanie informacji przez administratora w konkretnych przypadkach, w celu umożliwienia osobie, której dane są przetwarzane, wykonania przysługujących jej praw (art. 22 ust. 3 DODO)

Poniżej przykład klauzuli informacyjnej organu Policji na gruncie ochrony danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości



POLICJA MAZOWIECKA

DZIAŁANIA POLICJI | O POLICJI MAZOWIECKIEJ | PION PREWENCJI | RUCH DROGOWY | ZAMÓWIENIA

Strona główna / RODO/DODO

Rozmiar czcionki A A A

OCHRONA DANYCH OSOBOWYCH PRZETWARZANYCH W ZWIĄZKU Z ZAPOBIEGANIEM I ZWALCZANIEM PRZESTĘPCZOŚCI

Data publikacji 09.04.2019 Powrót Generuj PDF Drukuj

Szanowna Pani/Szanowny Panie, w związku z wejściem w życie: ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U z 2019 r., poz.125) dalej „ustawa wdrażająca dyrektywę 2016/680", dochowując warunków w niej zawartych informujemy, że:

1. **Administratorem** jest **Komendant Wojewódzki Policji z siedzibą w Radomiu**:
   - adres: ul. 11-go Listopada 37/59, 26-600 Radom,

2. Monitorowanie zgodności przetwarzania danych osobowych w Komendzie Wojewódzkiej Policji z siedzibą w Radomiu zapewnia **inspektor ochrony danych osobowych KWP z siedzibą w Radomiu**:

   Sylwia Fila
   - adres: ul. 11 Listopada 37/59, 26-600 Radom,
   - e-mail: iod.kwp@.ra.policja.gov.pl

3. Cel przetwarzania danych osobowych w Komendzie Wojewódzkiej Policji z siedzibą w Radomiu.

W KWP z siedzibą w Radomiu dane osobowe przetwarza się w celu rozpoznawania, zapobiegania, wykrywania i zwalczania czynów zabronionych, w tym zagrożeń dla bezpieczeństwa i porządku publicznego, a także wykonywania tymczasowego aresztowania, kar, kar porządkowych i środków przymusu skutkujących pozbawieniem wolności.

4. Prawa osób, których dane są przetwarzane zgodnie z ustawą wdrażającą dyrektywę 2016/680:
- prawo wniesienia do Prezesa Urzędu Ochrony Danych Osobowych lub innego organu sprawującego nadzór na podstawie przepisów odrębnych skargi w przypadku naruszenia praw osoby w wyniku przetwarzania jej danych osobowych,
- dane kontaktowe Prezesa Urzędu: ul. Stawki 2, 00-193 Warszawa, e-mail: iod@uodo.gov.pl,
- prawo żądania od administratora dostępu do danych osobowych, sprostowania lub usunięcia danych osobowych, lub ograniczenia przetwarzania danych osobowych dotyczących tej osoby, w sytuacjach przewidzianych prawem.

5.	**Wyznaczenie Inspektora Ochrony Danych**[129]	
	Administrator podmiot przetwarzający wyznaczają Inspektora Ochrony Danych w sytuacjach przewidzianych w art. 37 RODO	Zgodnie z art. 46 ustawy, każdy podmiot przetwarzający dane w celu rozpoznawania, zapobiegania, wykrywania i zwalczania czynów zabronionych, w tym zagrożeń dla bezpieczeństwa i porządku publicznego, a także wykonywania tymczasowego aresztowania, kar, kar porządkowych i środków przymusu skutkujących pozbawieniem wolności – a więc każdy z definicji administratora określonej w art. 4 ust. 1 – jest zobowiązany do powołania Inspektora Ochrony Danych

Źródło: opracowanie własne na podstawie *Kiedy stosujemy ustawę DODO – obowiązki z niej wynikające*, https://odo24.pl/blog-post.co-w-sytuacji-gdy-rodo-nie-ma-zastosowania-czyli-obowiazywanie-przepisow-ustawy-dodo, [dostęp: 17.07.2021] oraz *Klauzula informacyjna – ustawa DODO*, https://mazowiecka.policja.gov.pl/ra/rododo/29123,Ochrona-danych-osobowych-przetwarzanych-w-zwiazku-z-zapobieganiem-i-zwalczaniem-.html, [dostęp: 17.07.2021]

[129] Należy zwrócić uwagę na zależność, iż administratorzy danych zobowiązani do wyznaczenia IOD na podstawie ustawy najczęściej będą równolegle zobowiązani do wyznaczenie IOD na gruncie RODO, a zatem będą mogli wyznaczyć IOD na gruncie dwóch regulacji: art. 46 ustawy DODO oraz art. 37 ust. 1 RODO. Wynika to chociażby z faktu, że większość podmiotów podlegających pod ustawę o ochronie danych osobowych, przetwarzających dane w związku z zapobieganiem i zwalczaniem przestępczości to organy publiczne w rozumieniu art. 37 ust. 1 pkt 1 RODO (a więc zobowiązane do wyznaczenie IDO w oparciu o przepisy unijnego rozporządzenia). Wydaje się, że w takiej sytuacji administratorzy danych mogą wybrać jedną z dwóch możliwości: (a) powołać dwóch odrębnych inspektorów, lub też (b) przypisać zadania zarówno z ustawy DODO jak i RODO jednemu IOD. Możliwość wyznaczenia dwóch IOD potwierdzają chociażby odrębne formularze rejestracyjne IOD przy Prezesie Urzędu Ochrony Danych Osobowych. Zob. *Kiedy stosujemy ustawę DODO – obowiązki z niej wynikające*, https://odo24.pl/blog-post.co-w-sytuacji-gdy-rodo-nie-ma-zastosowania-czyli-obowiazywanie-przepisow-ustawy-dodo, [dostęp: 17.07.2021].

Zakres materialnoprawny ustawy dopełnia rozporządzenie Prezesa Rady Ministrów z dnia 31 maja 2019 r. w sprawie trybu i sposobu realizacji zadań przez inspektora ochrony danych, które doprecyzowuje sposób funkcjonowania Inspektora Ochrony Danych w sektorze organów zajmujących się zapobieganiem i zwalczaniem przestępczości, w szczególności formę i sposób realizacji zadań, o których mowa w art. 47 ust. 1 pkt 1–9 ustawy[130].

Podobnie jak w przypadku ustawy z 10 maja 2018 roku, ustawa przewiduje także kary za przetwarzanie danych, gdy do ich przetwarzania podmiot nie jest uprawniony lub gdy udaremnia, lub istotnie utrudnia przeprowadzenie kontroli przez Prezesa UODO. Są nimi: grzywna, kara ograniczenia wolności albo pozbawienie wolności do dwóch lat. Jeżeli czyn dotyczy danych wrażliwych, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat trzech[131].

Strukturę modelu ochrony danych osobowych przetwarzanych w związku ze zwalczaniem transgranicznej przestępczości dopełnia tzw. system PNR (*Passenger Name Record*), tj. mechanizm gromadzenia przez przewoźników lotniczych danych dotyczących przelotu pasażera oraz ich przetwarzania do celów zapobiegania przestępstwom terrorystycznym oraz poważnej przestępczości[132]. „System PNR uzupełnia już funkcjonujące narzędzia zwalczania przestępczości transgranicznej. Przewoźnicy lotniczy muszą przekazywać dane PNR dotyczące lotów przychodzących i wychodzących z UE. Państwa członkowskie mogą też, ale nie muszą, gromadzić dane PNR dotyczące wybranych lotów wewnątrzunijnych (…). Przetwarzanie danych PNR pozwala organom ścigania identyfikować osoby wcześniej nie podejrzewane o związki z przestępczością lub terroryzmem, zanim szczegółowa analiza danych wykaże, że osoby te posiadają takie związki"[133].

Na poziomie wspólnotowym dostrzeżono zatem banalne powiązanie między terroryzmem i przestępczością transgraniczną a podróżami międzynarodowymi. Z uwagi na wdrożone, w ramach systemu Schengen, środki rekompensujące zniesienie kontroli na granicach, większość państw członkowskich UE korzystała już z danych dot. pasażerów lotniczych na mocy przepisów prawa krajowego[134]. Ujednolicenie na szczeblu unijnym trybu pozyskiwania danych przez organy krajowe państw członkowskich natomiast dokonało się dyrektywą Parlamentu Europejskiego i Rady (UE) 2016/681 z dnia 27 kwietnia 2016 r. w sprawie wykorzystywania danych dotyczących przelotu pasażera (danych PNR) w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań

[130] Zob. rozporządzenie Prezesa Rady Ministrów z dnia 31 maja 2019 r. w sprawie trybu i sposobu realizacji zadań przez inspektora ochrony danych (Dz.U. z 2019 r., poz. 1041).

[131] Rozdział 8 ustawy z dnia 14 grudnia 2018 roku o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. z 2019 r., poz. 125).

[132] Dane PNR można wykorzystywać m.in.: (a) do oceny pasażerów przed przylotem lub wylotem według określonych kryteriów ryzyka lub do identyfikacji konkretnych osób, (b) do opracowywania takich kryteriów ryzyka, (c) w konkretnych dochodzeniach lub postępowaniach sądowych. Szerzej zob. Komunikat Komisji w sprawie globalnego podejścia do przekazywania danych dotyczących przelotu pasażera (PNR) państwom trzecim, KOM(2010) 492 wersja ostateczna, Bruksela 21.09.2010 r.

[133] *Kontrola nad danymi o przelocie pasażera (PNR)*, Rada Europejska, https://www.consilium.europa.eu/pl/policies/fight-against-terrorism/passenger-name-record/, [dostęp: 22.07.2021].

[134] Szerzej na temat zob. Opinia 07/2010 dotycząca komunikatu Komisji w sprawie globalnego podejścia do przekazywania danych dotyczących przelotu pasażera (PNR) państwom trzecim, WP 178, przyjęta 12 listopada 2010, Grupa robocza art. 29. Por. Rezolucja Parlamentu Europejskiego z 11.11.2010 r. w sprawie globalnego podejścia do przekazywania krajom trzecim danych dotyczących przelotu pasażera (PNR) oraz zaleceń Komisji dla Rady dotyczących upoważnienia do podjęcia negocjacji między Unią Europejską a Australią, Kanadą i Stanami Zjednoczonymi, P7_TA(2010)0397.

przygotowawczych w ich sprawie i ich ścigania[135] Potrzeba wprowadzenia uregulowań wiązała się również z zawarciem przez UE umów międzynarodowych wprowadzających obowiązek przekazywania danych PNR władzom państw trzecich[136] (USA[137], Australii[138], Kanady[139] czy Japonii[140]). W Polsce transpozycję ww. dyrektywy[141] przeprowadzono ustawą z dnia 9 maja 2018 roku o przetwarzaniu danych dotyczących przelotu pasażera[142], która (jak w treści aktu) określiła zasady i warunki przekazywania przez przewoźników lotniczych danych dotyczących przelotu pasażera oraz przetwarzania tych danych w celu zapobiegania, wykrywania i zwalczania przestępstw o charakterze terrorystycznym, skarbowych i innych oraz ścigania ich sprawców.

Ustawa nakłada obowiązek nieodpłatnego przekazywania do Krajowej Jednostki do spraw Informacji o Pasażerach (JIP) danych PNR na przewoźników lotniczych organizujących loty PNR. Zgodnie ze ustawowym słownikiem definicyjnym dane PNR obejmują dane dotyczące przelotu pasażera, w tym dane osobowe, które są przetwarzane w związku z prowadzeniem działalności gospodarczej przez przewoźników lotniczych w celu dokonania rezerwacji lub realizacji lotu w ramach przewozu lotniczego, podlegające przekazaniu przez przewoźnika lotniczego do JIP. Z kolei lot PNR oznacza lot statku powietrznego wykonującego przewóz lotniczy pasażerów, podczas którego następuje przekroczenie granicy państwowej, a start albo lądowanie statku powietrznego następuje na terytorium Rzeczypospolitej Polskiej. Natomiast przetwarzanie danych PNR to operacje wykonywane na danych PNR, takie jak: gromadzenie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie przez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie[143].

Przewoźnicy lotniczy przekazują samoczynnie (tzw. bez wezwania do tego) polskiej Straży Granicznej będące w ich posiadaniu dane PNR, dotyczące każdego z planowanych przez siebie lotów, dwukrotnie we wskazanych w ustawie terminach, tj.:

---

135 Dz. Urz. UE L 132 z 4.5.2016, s. 119.

136 UE podpisała już umowy pozwalające unijnym przewoźnikom przekazywać dane pasażera do USA, Kanady i Australii. W lutym 2020 r. Rada przyjęła decyzję upoważniającą do rozpoczęcia negocjacji w sprawie podobnej umowy z Japonią. Zob. Rezolucja Parlamentu Europejskiego z dnia 5 maja 2010 r. dotycząca rozpoczęcia negocjacji w sprawie umów dotyczących rejestru nazwisk pasażerów (PNR) ze Stanami Zjednoczonymi, Australią i Kanadą, 2011/C 81 E/12 (Dz.Urz. UE C z dnia 15.3.2011 r.).

137 Zob. Umowa między USA a UE o wykorzystywaniu danych dot. przelotu pasażera (PNR) praz przekazywania takich danych do Departamentu Bezpieczeństwa Wewnętrznego USA (Dz.Urz. UE L 215 z 11.6.2012 r.). Por. Umowa między Unią Europejską a Stanami Zjednoczonymi Ameryki o przetwarzaniu i przekazywaniu przez przewoźników lotniczych danych dotyczących przelotu pasażera (PNR) do Departamentu Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych (Dz. Urz. UE L 298 z 2006 r.), (akt uchylony).

138 Umowa między UE a Australią o przetwarzaniu i przekazywaniu przez przewoźników lotniczych australijskiej służbie celnej danych PNR pochodzących z UE (Dz.Urz. UE L 213 z 8.8.2008 r.).

139 Zob. (a) Umowa między Wspólnotą Europejską a Rządem Kanady o przetwarzaniu zaawansowanych informacji o pasażerach oraz zapisu danych dotyczących nazwiska pasażera (Dz. Urz. UE L 82 z 21.3.2006, s. 15), (b) Decyzja Rady z dnia 18 lipca 2005 r. w sprawie zawarcia Umowy pomiędzy Wspólnotą Europejską a Rządem Kanady o przetwarzaniu danych API/PNR (2006/230/WE), (Dz. Urz. UE L 82 z 21.3.2006, s. 14).

140 Decyzja Rady upoważniająca do rozpoczęcia negocjacji z Japonią w sprawie umowy między Unią Europejską a Japonią o przekazywaniu i wykorzystywaniu danych dotyczących przelotu pasażera (PNR) w celu zapobiegania terroryzmowi i poważnym przestępstwom transgranicznym oraz walki z nimi, 5378/20, Bruksela 4 lutego 2020 r.

141 W grudniu 2015 roku Parlament Europejski i Rada osiągnęły porozumienie co do tekstu kompromisowego, 14 kwietnia 2016 roku Parlament Europejski przyjął swoje stanowisko, 21 kwietnia 2016 roku dyrektywę przyjęła Rada, a państwa członkowskie miały 2 lata, by wprowadzić w życie przepisy ustawowe, wykonawcze i administracyjne niezbędne do wykonania dyrektywy. Zob. *Kontrola nad danymi o przelocie pasażera (PNR)*, Rada Europejska, https://www.consilium.europa.eu/pl/policies/fight-against-terrorism/passenger-name-record/, [dostęp: 22.07.2021].

142 Dz.U. z 2019 r., poz. 1783.

143 Odpowiednio art. 2 pkt 1, 6 i 10 ustawy z dnia 9 maja 2018 r. o przetwarzaniu danych dotyczących przelotu pasażera (Dz.U. z 2019 r., poz. 1783).

1) od 48 do 24 godzin przed planowanym rozpoczęciem lotu PNR,
2) niezwłocznie po zakończeniu odprawy biletowo-bagażowej i wejściu wszystkich pasażerów na pokład statku powietrznego (kiedy nie można już opuścić pokładu przed startem, a inni pasażerowie nie mogą już wejść), przy czym w przypadku przewozu ad hoc, wystarczy tylko raz, tj. niezwłocznie po zakończeniu odprawy biletowo-bagażowej.

Ponadto Straż Graniczna może wystąpić do przewoźnika lotniczego o przekazanie danych PNR (na wcześniejszy wniosek jednego z uprawnionych organów) niezależnie od wskazanych powyżej terminów, przy czym wniosek może złożyć nawet ustnie, a następnie niezwłocznie potwierdzić go w formie pisemnej w postaci papierowej lub elektroniczne[144]. W takim wypadku organ może (ale nie musi) zwolnić przewoźnika lotniczego od przekazania danych PNR w terminie wynikającym z ustawy. Przewoźnik lotniczy powinien przekazywać dane za pomocą środków komunikacji elektronicznej, przy wykorzystaniu protokołów oraz formatów danych określonych w przepisach wykonawczych do ustawy[145]. Katalog przekazywanych danych został precyzyjnie określony w ustawie. Należą do nich m.in.:

1) data dokonania rezerwacji lub wystawienia biletu,
2) data przelotu,
3) imię i nazwisko pasażera oraz jego dane teleadresowe,
4) informacje dotyczące płatności za bilet,
5) numer miejsca na pokładzie statku powietrznego,
6) informacje dotyczące bagażu,
7) obywatelstwo, płeć i pozostałe dane wynikające z dokumentu tożsamości.

Z uwagi na ochronę praw podstawowych z katalogu wyłączono dane wrażliwe ujawniające: rasę, pochodzenie etniczne, poglądy polityczne, przekonanie religijne lub światopoglądowe, przynależność do związków zawodowych, stan zdrowia, życie seksualne lub orientację seksualną danej osoby. Okres retencji pozyskanych danych określono na 5 lat, przy czym po 6 miesiącach należy dokonać anonimizacji danych, tak by uniemożliwić identyfikację osoby, której dotyczą.

Należy mieć na uwadze, że niektórzy przewoźnicy lotniczy, w ramach gromadzenia i przetwarzania danych PNR, w związku z zwalczaniem nielegalnej imigracji i ulepszeniem

[144] Od tej zasady ustawa PNR przewiduje dwa wyjątki. Przewoźnik lotniczy wykonujący nieregularny przewóz lotniczy pasażerów może pisemnie uzgodnić ze Strażą Graniczną inny sposób przekazywania danych PNR za pomocą środków komunikacji elektronicznej, jeśli nie dysponuje infrastrukturą umożliwiającą obsługę protokołów i formatów danych określonych w przepisach wykonawczych. Również gdy z powodu awarii technicznej nie jest możliwe przekazywanie danych w dotychczasowy sposób, przewoźnik lotniczy może ustalić ze Strażą Graniczną sprawny sposób przekazywania. Poza danymi PNR przewoźnik lotniczy musi dodatkowo przekazać Straży Granicznej informacje dotyczące niego samego oraz prowadzonej przez niego działalności na terenie Polski, w tym ustalonych rozkładów lotów oraz programów lotów, a także gromadzonych przez siebie kategorii danych PNR. Jest to tzw. obowiązek informacyjny przewoźników lotniczych. Informacje te należy przekazać jednokrotnie, w formie pisemnej (w postaci papierowej lub dokumentu elektronicznego), co do zasady w terminie do 14 dni przed rozpoczęciem wykonywania lotów międzynarodowych. Aktualizacji przekazanych już informacji przewoźnik lotniczy powinien natomiast dokonać bezzwłocznie. Zob. M. Sobkowicz, *Kary za nieprzekazanie danych dotyczących przelotu pasażera (PNR)*, https://codozasady.pl/p/kary-za-nieprzekazanie-danych-dotyczacych-przelotu-pasazera-pnr-, [dostęp: 22.07.2021].

[145] Zob. rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 22 maja 2018 r. w sprawie określenia protokołów i formatów danych wykorzystywanych przez przewoźników lotniczych w celu przekazywania danych PNR do Krajowej Jednostki do spraw Informacji o Pasażerach (Dz.U. z 2018 r., poz. 1012). Por. rozporządzenie Rady Ministrów z dnia 30 maja 2018 r. w sprawie przetwarzania danych dotyczących przelotu pasażera przez Krajową Jednostkę do spraw Informacji o Pasażerach (Dz.U. z 2018 r., poz. 1148).

kontroli granicznej, mają również obowiązek zatrzymać (jako ich część), zebrane przez nich zaawansowane informacje o pasażerach, tj. dane API (*Advance Passenger Information*). Obowiązek przewoźników, wynikający z dyrektywy 2004/82/WE z dnia 29 kwietnia 2004 r. w sprawie zobowiązania przewoźników do przekazywania danych pasażerów (dyrektywa API)[146], ogranicza się jednak wyłącznie do lotów z/do państw trzecich, a dane udostępniane są na wniosek organów (tj. za pomocą metody „*pull*", co odróżnia dane API od PNR, które są głównie pozyskiwane metodą „*push*"). Dane przekazywane na wniosek obejmują:

1) imię lub imiona oraz nazwisko w pełnym brzmieniu,
2) datę urodzenia,
3) numer i rodzaj dokumentu podróży,
4) obywatelstwo,
5) nazwę przejścia granicznego, w którym nastąpi przekroczenie granicy RP,
6) numer lotu,
7) datę i czas startu i lądowania statku powietrznego,
8) liczbę pasażerów statku powietrznego,
9) lotnisko wejścia pasażera na pokład statku powietrznego w celu odbycia lotu[147].

Dane API powinny być przekazane po zakończeniu odprawy bagażowej i nie później niż w chwili startu. Komendant SG usuwa dane po zakończeniu kontroli granicznej pax danego lotu, jednak nie później niż po upływie 24 godzin od chwili przekazania informacji przez przewoźnika w odpowiednim formacie technicznym[148]. „Wykorzystywanie danych PNR wraz z danymi API stanowi wartość dodaną w zakresie pomocy państwom członkowskim w weryfikacji tożsamości osób, zwiększając tym samym przydatność wyników tych działań dla ścigania przestępczości i minimalizując ryzyko dokonywania sprawdzeń i prowadzenia postępowań przygotowawczych w stosunku do osób niewinnych"[149].

Przewoźnicy lotniczy, obok obowiązku informacyjnego względem organów publicznych, na okoliczność gromadzenia i przetwarzania danych osobowych podróżnych, muszę zrealizować obowiązek informacyjny również względem osób, których dane dotyczą. Przepisy PNR nakładają w tym zakresie dodatkowy – obok RODO – szczegółowy zakres klauzuli informacyjnej[150].

[146] Dz.Urz. UE L 261 z 6.8. 2004 r., s. 24–27. W Polsce dyrektywa 2004/82/WE (API) została implementowana m.in. przepisami art. 202a-202d, 209u ustawy z dnia 3 lipca 2002 r. Prawo lotnicze (Dz.U. z 2002 r. Nr 130, poz. 1112 z późn. zm.).
[147] Art. 202a ust. 3 ustawy z dnia 3 lipca 2002 r. Prawo lotnicze (Dz.U. z 2002 r. Nr 130, poz. 1112 z późn. zm.).
[148] Zob. Rozporządzenie Ministra Spraw Wewnętrznych z dnia 24 października 2012 r. w sprawie wymagań technicznych i organizacyjnych dotyczących przekazywania Straży Granicznej informacji przez przewoźników lotniczych (Dz. U. z 2012 r., poz. 1249). Por. Opinia nr 9/2006 dotycząca wdrożenia dyrektywy 2004/82/WE Rady w sprawie zobowiązania przewoźników do przekazywania z wyprzedzeniem danych pasażerów, (WP 127), przyjęta 28 września 2006 r., Grupa Robocza art. 29.
[149] T. Balcerzak, *Bezpieczny lot, bezpieczne dane*, http://www.europedirect.um.warszawa.pl/aktualnosci/bezpieczny-lot-bezpieczne-dane, [dostęp: 5.10.2021].
[150] Zob. motyw 29, 37 oraz art. 13 dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/681 z dnia 27 kwietnia 2016 r. w sprawie wykorzystywania danych dotyczących przelotu pasażera (danych PNR) w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania (Dz.Urz. UE L 119 z 4.5.2016, s. 132–149).

TABELA 7 Informacja o przetwarzaniu danych osobowych w ramach wykonywania umowy przewozu zawartej pomiędzy pasażerem a PLL LOT S.A.

Przetwarzanie danych dotyczących przelotu pasażera (PNR) – klauzula informacyjna
Podane w rezerwacji dane dotyczące przelotu pasażera (PNR) są przekazywane na podstawie przepisów ustawy z dnia 9 maja 2018 r. o przetwarzaniu danych dotyczących przelotu pasażera przez PLL LOT S.A. na rzecz Krajowej Jednostki ds. Informacji o Pasażerach (JIP) w celu wykrywania i zwalczania przestępstw o charakterze terrorystycznym i innych przestępstw lub przestępstw skarbowych oraz zapobiegania im i ścigania ich sprawców. Dane PNR są przekazywane przez przewoźników lotniczych do JIP w następujących terminach: a) od 48 do 24 godzin przed planowanym rozpoczęciem lotu oraz b) niezwłocznie po zakończeniu odprawy biletowo-bagażowej i wejściu pasażerów na pokład statku powietrznego, kiedy nie mogą już go opuścić przed jego startem, a inni pasażerowie nie mogą wejść na pokład. Przewoźnik lotniczy przekazuje dane PNR do JIP za pomocą środków komunikacji elektronicznej. Dane PNR są przechowywane przez JIP przez 5 lat od dnia ich zgromadzenia, a po upływie tego okresu podlegają niezwłocznie trwałemu usunięciu. W trybie wnioskowym dane PNR mogą być przekazane na rzecz Krajowej Jednostki do spraw Informacji o Pasażerach państwa członkowskiego innego niż Rzeczpospolita Polska. W związku z przekazywaniem danych PNR przysługują Ci następujące uprawnienia: a) prawo dostępu do danych osobowych, b) żądania ich uzupełnienia, uaktualnienia, sprostowania lub usunięcia, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zgromadzone z naruszeniem prawa, c) prawo do odszkodowania oraz dochodzenia swoich praw na drodze sądowej, w przypadku naruszenia zasad przetwarzania jego danych osobowych przez JIP, d) prawo do kontaktu z Inspektorem do spraw ochrony danych o pasażerach za pośrednictwem numeru telefonu: +48 22 513 54 87 lub adresu e-mail: inspektor-PNR@strazgraniczna.pl, e) prawo do złożenia wniosku o udzielenie informacji o przysługujących prawach, f) prawo do złożenia skargi do Prezesa Urzędu Ochrony Danych Osobowych w zakresie przetwarzania danych osobowych pasażera w związku z przetwarzaniem danych PNR.
Administratorem danych PNR przekazanych do JIP jest Komendant Główny Straży Granicznej al. Niepodległości 100, 02–514 Warszawa, telefon: +48 22 500 40 00, e-mail: gabinet.kg@strazgraniczna.pl

Źródło: *Informacja o przetwarzaniu danych osobowych w ramach wykonywania umowy przewozu zawartej pomiędzy pasażerem a PLL LOT S.A.*, https://www.lot.com/cz/pl/ochrona-danych-osobowych/klauzula-informacyjna-przewoz, [dostęp: 22.07.2021]

Za niedopełnienie obowiązków wynikających z ustawy PNR, na przewoźnika lotniczego mogą zostać nałożone administracyjne kary pieniężne w zryczałtowanej wysokości. Kara nakładana jest oddzielnie za każdy lot oraz w odniesieniu do każdego z terminów, w którym dany przewoźnik lotniczy był zobowiązany do przekazania danych PNR, co oznacza możliwość sumowania kar (system jest sztywny, nie zależy od stopnia zawinienia, wielkości i charakteru przewoźnika oraz nie podlega miarkowaniu). Nałożenie kary administracyjnej następuje natomiast w formie decyzji administracyjnej Komendanta Głównego Straży Granicznej, która może zostać wydana w terminie 3 lat od dnia, w którym przewoźnik lotniczy dopuścił się naruszenia[151]. Ukarany może wystąpić z wnioskiem o ponowne rozpatrzenie sprawy albo wnieść skargę do sądu administracyjnego. Przewoźnik lotniczy, który: (1) nie przekazuje danych PNR do JIP w terminie podlega administracyjnej karze pieniężnej w wysokości 20 000 zł, natomiast ten, który (2) nie przekazuje do JIP wszystkich zgromadzonych, w celu dokonania rezerwacji lub realizacji lotu PNR, elementów kategorii danych PNR, do których przekazania był zobowiązany, podlega administracyjnej karze pieniężnej w wysokości 12 000 zł – za każdy lot PNR, w którym takie naruszenie nastąpiło. Przewoźnik lotniczy, który nie przekazuje danych PNR w formacie danych zgodnym z formatem określonym w przepisach wykonawczych albo za pomocą środków komunikacji elektronicznej

[151] Art. 67–70 ustawy z dnia 9 maja 2018 r. o przetwarzaniu danych dotyczących przelotu pasażera (Dz.U. z 2019r., poz. 1783). Zgodnie z informacjami prasowymi 210 przewoźników lotniczych, którzy od 2018 roku (w latach 2018–2020 wykonano prawie 940 000 operacji lotniczych związanych z przewozem pasażerów – zarówno na trasach krajowych, jak i międzynarodowych) wykonywali przewozy lotnicze na trasach do Polski i z Polski, stało się stroną postępowań w przedmiocie nałożenia kary administracyjnej. Komendant Główny Straży Granicznej wszczął wobec nich w sumie około 17 tysięcy postępowań na łączna kwotę kar nawet 640 milionów złotych. I. Kacprzak, *Kary podetną skrzydła*, https://archiwum.rp.pl/artykul/1459898-Kary-podetna-skrzydla.html, [dostęp: 5.10.2021].

uzgodnionych z Komendantem Głównym Straży Granicznej podlega administracyjnej karze pieniężnej w wysokości 16 000 zł za każdy lot PNR, w którym takie naruszenie nastąpiło. Najwyższa kara, jaka może zostać nałożona na przewoźnika lotniczego w związku z jednym lotem PNR, nie może przekroczyć 40 000 zł. Ponadto za niedopełnienie opisanego wyżej obowiązku informacyjnego (nieprzekazanie informacji w terminie wynikającym z ustawy lub brak ich niezwłocznej aktualizacji) może zostać nałożona na przewoźnika lotniczego kara 5 000 zł. Kary mogą być zmniejszone o 50%, jeśli przewoźnik lotniczy usunie skutki swojego naruszenia, czyli przekaże dane PNR w dodatkowych określonych w ustawie terminach (w zależności od rodzaju naruszenia – do 6 godzin przed startem lub do czasu lądowania)[152].

TABELA 8 Kary administracyjne za nieprzekazanie danych PNR

	Nieprzekazanie danych PNR za jeden lot PNR	
	zgodnie z wymogami ustawy PNR	na wniosek Straży Granicznej
nieprzekazanie w ogóle lub nie w terminie	20 000 zł	10 000 zł
nie wszystkie posiadane kategorie danych	12 000 zł	6 000 zł
nie w sposób zgodny z ustawą PNR	16 000 zł	8 000 zł

Źródło: M. Sobkowicz, *Kary za nieprzekazanie danych dotyczących przelotu pasażera (PNR)*, https://codozasady.pl/p/kary-za-nieprzekazanie-danych-dotyczacych-przelotu-pasazera-pnr-, [dostęp: 22.07.2021]

Termin wykonania administracyjnych kar pieniężnych, wynosi 30 dni od dnia, w którym decyzja w sprawie nałożenia kary stała się ostateczna. Należności z tytułu administracyjnych kar pieniężnych podlegają egzekucji w trybie przepisów ustawy o postępowaniu egzekucyjnym w administracji[153], przy czym należy mieć na uwadze nowelizację ustawy PNR, mającą pomóc branży lotniczej w związku z pandemią[154]. Przewoźnik lotniczy nie podlega karze pieniężnej w przypadku, gdy niedopełnienie obowiązku nastąpiło w wyniku:

- działania siły wyższej,
- awarii systemu służącego SG do pozyskiwania oraz przetwarzania danych PNR,
- awarii powstałej po stronie przewoźnika lotniczego [155].

[152] Art. 64–66 ustawy z dnia 9 maja 2018 r. o przetwarzaniu danych dotyczących przelotu pasażera (Dz.U. z 2019r., poz. 1783).
[153] Art. 68–73 ustawy o przetwarzaniu danych dotyczących przelotu pasażera (Dz.U. z 2019r., poz. 1783).
[154] Rada Ministrów w dniu 7 grudnia 2021 roku przyjęła projekt zmian w ustawie PNR.. W szczególności nowelizacja wprowadziła możliwość rozłożenia w czasie nakładania na przewoźników lotniczych administracyjnych kar finansowych. Ograniczone zostały także niektóre obowiązki administracyjne. Zgodnie z nowelizacją okresy przedawnienia będą ustalane w oparciu o przepisy, które będą obowiązywały w dniu przedawnienia. Wprowadzono możliwość nakładania administracyjnych kar pieniężnych nie tylko przez KGSG, ale także przez komendanta oddziału SG. Jednocześnie umożliwiono objęcie jednym postępowaniem więcej niż jednego naruszenia i wydania jednej decyzji w odniesieniu do wielu naruszeń. Zob. *Rząd przyjął projekt zmian w ustawie o przetwarzaniu danych dotyczących przelotu pasażera*, https://www.gov.pl/web/mswia/rzad-przyjal-projekt-zmian-w-ustawie-o-przetwarzaniu-danych-dotyczacych-przelotu-pasazera, [dostęp: 22.07.2021]. Por. *Sejm znowelizował ustawę o przetwarzaniu danych, dotyczących przelotu* pasażera, https://inwestycje.pl/gospodarka/sejm-znowelizowal-ustawe-o-przetwarzaniu-danych-dotyczacych-przelotu-pasazera/, [dostęp: 22.07.2021].
[155] Art. 69 ustawy z 9 o przetwarzaniu danych dotyczących przelotu pasażera (Dz.U. z 2019 r., poz. 1783).

W przypadku danych API, zgodnie z dyrektywą 2004/82/WE, państwa członkowskie podejmują niezbędne środki, aby zapewnić, że sankcje na przewoźników są odstraszające, skuteczne i proporcjonalne oraz że: (a) maksymalna wysokość takich sankcji jest nie mniejsza niż 5.000 EUR lub ekwiwalent w walucie krajowej, albo (b) minimalna wysokość takich sankcji jest nie mniejsza niż 3.000 EUR lub niż ekwiwalent w walucie krajowej[156]. Przewoźnik lotniczy, który wbrew obowiązkowi:

1) nie przekazał informacji – podlega karze pieniężnej w wysokości 22 500 zł.,
2) przekazał informację nieprawdziwą – podlega karze w wysokości 18 000 zł.,
3) przekazał informację niepełną – podlega karze pieniężnej w wysokości 13 500 zł.

– za każdy lot, w którym odpowiednio nie przekazał informacji, przekazał informację nieprawdziwą lub przekazał informację niepełną. Kary pieniężne, na wniosek komendanta placówki Straży Granicznej właściwego ze względu na miejsce przekroczenia granicy przez pasażerów statku powietrznego, wymierza Prezes Urzędu Lotnictwa Cywilnego[157].

Wybrane zmiany sektorowe

Aby zapewnić skuteczne stosowanie przepisów RODO, poza uchwaleniem ustawy o ochronie danych osobowych, konieczne było także dokonanie zmian w istniejących już przepisach. W szczególności należy uwzględnić w tym zakresie dwie nowelizację ustawy o ochronie danych osobowych, które weszły w życie 1 października 2018[158] roku oraz 4 maja 2019 roku[159]. Pierwsza z nich wprowadziła do ustawy korekty w zakresie podmiotów zgłaszających kandydatów do Rady do Spraw Ochrony Danych Osobowych (których mogą zgłaszać osoby, o których mowa w art. 7 ust. 1 pkt 1, 2 i 4–6 ustawy z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce) oraz kosztów poniesionych przez Policję z tytułu udzielonej pomocy przy wykonywaniu czynności kontrolnych (stawka zryczałtowana w wysokości 1,5% przeciętnego miesięcznego wynagrodzenia w sektorze przedsiębiorstw).

Druga nowelizacja stanowiła właśnie kompleksowe uzupełnienie samej ustawy poprzez wprowadzenie postanowień regulujących materię ochrony danych osobowych w szeregu obszarów materialnoprawnych, łącznie w 162 aktach prawnych – albo poprzez dodanie do ustawy sektorowej rozdziału zatytułowanego: „Przetwarzanie danych osobowych"[160], albo poprzez wprowadzenie dedykowanych danej ustawie zmian[161]. Jak wskazano w uzasadnieniu

[156] Art. 4 dyrektywy 2004/82/WE z dnia 29 kwietnia 2004 r. w sprawie zobowiązania przewoźników do przekazywania danych pasażerów (dyrektywa API), (Dz.Urz. UE L 261 z 6.8.2004 r., s. 24–27).
[157] Art. 209u ustawy z dnia 3 lipca 2002 r. Prawo lotnicze (Dz.U. 2002 nr 130 poz. 1112 z późn. zm.).
[158] Ustawa z dnia 3 lipca 2018 r. – Przepisy wprowadzające ustawę – Prawo o szkolnictwie wyższym i nauce (Dz.U. 2018 poz. 1669).
[159] Ustawa z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania 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), (Dz.U. 2019 poz. 730).
[160] Tak w ustawach: (1) o izbach morskich, (2) Prawo o adwokaturze, (3) o radcach prawnych, (4) Prawo o notariacie, (5) Prawo o ruchu drogowym, (6) o usługach detektywistycznych, (7) o świadczeniu przez prawników zagranicznych pomocy prawnej w Rzeczypospolitej Polskiej, (8) o zawodzie tłumacza przysięgłego.
[161] Tak w ustawach: (1) Kodeks postępowania administracyjnego, (2) o postępowaniu egzekucyjnym w administracji, (3) Kodeks pracy, (4) Karta Nauczyciela, (5) o księgach wieczystych i hipotece, (6) Prawo spółdzielcze, (7) o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi, (8) o narodowym zasobie archiwalnym i archiwach, (9) o drogach publicznych, (10) o rybactwie śródlądowym, (11) o Rzeczniku Praw Obywatelskich, (12) Prawo geodezyjne i kartograficzne, (13) o obszarach morskich Rzeczypospolitej Polskiej i administracji morskiej, (14) o rozwiązywaniu sporów zbiorowych, (15) o Inspekcji Ochrony Środowiska, (16) o ochronie przeciwpożarowej, (17) o Państwowej Straży Pożarnej, (18) o systemie oświaty, (19) o organizowaniu

do projektu ustawy celem nowelizacji było dostosowanie polskiego porządku prawnego do RODO m.in. przez usunięcie przepisów, które są nim sprzeczne lub powielają jego rozwiązania.

Z punktu widzenia powszechności obrotu społeczno-ekonomicznego za najważniejsze należy uznać zmiany regulujące materię: (a) prawa pracy i spraw kadrowych, (b) działań telemarketingowych, czy (c) zamówień publicznych. Z uwagi na ważkość aktu, oddzielnie należy potraktować nowelizację Kodeksu postępowania administracyjnego[162]. I tak koncentrując się jedynie na najważniejszych zmianach należy odnotować jak następuje.

---

i prowadzeniu działalności kulturalnej, (20) o orderach i odznaczeniach, (21) o zaopatrzeniu emerytalnym żołnierzy zawodowych oraz ich rodzin, (22) o zaopatrzeniu emerytalnym funkcjonariuszy Policji, Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego, Centralnego Biura Antykorupcyjnego, Straży Granicznej, Służby Ochrony Państwa, Państwowej Straży Pożarnej, Służby Celno-Skarbowej i Służby Więziennej oraz ich rodzin, (23) o zakładowym funduszu świadczeń socjalnych, (24) Prawo budowlane, (25) o ochronie zdrowia psychicznego, (26) o autostradach płatnych oraz o Krajowym Funduszu Drogowym, (27) o statystyce publicznej, (28) o zasadach ewidencji i identyfikacji podatników i płatników, (29) Prawo łowieckie, (30) o osobach deportowanych do pracy przymusowej oraz osadzonych w obozach pracy przez III Rzeszę i Związek Socjalistycznych Republik Radzieckich, (31) o doradztwie podatkowym, (32) o Radzie Ministrów, (33) o utrzymaniu czystości i porządku w gminach, (34) o zawodach lekarza i lekarza dentysty, (35) Prawo energetyczne, (36) Kodeks karny, (37) o publicznej służbie krwi, (38) o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych, (39) Ordynacja podatkowa, (40) o Narodowym Banku Polskim, (41) Prawo bankowe, (42) o systemie ubezpieczeń społecznych, (43) o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych, (44) o Rzeczniku Praw Dziecka, (45) o Krajowym Rejestrze Karnym, (46) Prawo atomowe, (47) o funkcjonowaniu banków spółdzielczych, ich zrzeszaniu się i bankach zrzeszających, (48) o samorządach zawodowych architektów oraz inżynierów budownictwa, (49) o żegludze śródlądowej, (50) o ochronie dziedzictwa Fryderyka Chopina, (51) o kuratorach sądowych, (52) o szczególnych zasadach odbudowy, remontów i rozbiórek obiektów budowlanych zniszczonych lub uszkodzonych w wyniku działania, (53) o Żandarmerii Wojskowej i wojskowych organach porządkowych, (54) o transporcie drogowym, (55) Prawo lotnicze, (56) o świadczeniu usług drogą elektroniczną, (57) o planowaniu i zagospodarowaniu przestrzennym, (58) o transporcie kolejowym, (59) o ubezpieczeniach obowiązkowych, Ubezpieczeniowym Funduszu Gwarancyjnym i Polskim Biurze Ubezpieczycieli Komunikacyjny, (60) o zatrudnieniu socjalnym, (61) o ochronie zabytków i opiece nad zabytkami, (62) o służbie wojskowej żołnierzy zawodowych, (63) o wykonywaniu prac podwodnych, (64) o świadczeniach rodzinnych, (65) Prawo zamówień publicznych, (66) o pomocy społecznej, (67) o wyrobach budowlanych, (68) o promocji zatrudnienia i instytucjach rynku pracy, (69) o świadczeniach przedemerytalnych, (70) o postępowaniu w sprawach dotyczących pomocy publicznej, (71) o funduszach inwestycyjnych i zarządzaniu alternatywnymi funduszami inwestycyjnymi, (72) Prawo telekomunikacyjne, (73) o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych, (74) o odpowiedzialności za naruszenie dyscypliny finansów publicznych, (75) o informatyzacji działalności podmiotów realizujących zadania publiczne, (76) o opłatach abonamentowych, (77) o przeciwdziałaniu przemocy w rodzinie, (78) o obrocie instrumentami finansowymi, (79) o dokumentach paszportowych, (80) o nadzorze nad rynkiem finansowym, (81) o biokomponentach i biopaliwach ciekłych, (82) o Państwowym Ratownictwie Medycznym, (83) o drogowych spółkach specjalnego przeznaczenia, (84) o zarządzaniu kryzysowym, (85) o licencji doradcy restrukturyzacyjnego, (86) o pomocy osobom uprawnionym do alimentów, (87) o zmianie imienia i nazwiska, (88) o prawach pacjenta i Rzeczniku Praw Pacjenta, (89) o służbie cywilnej, (90) o Krajowej Szkole Sądownictwa i Prokuratury, (91) o obywatelstwie polskim, (92) o zadośćuczynieniu rodzinom ofiar zbiorowych wystąpień wolnościowych w latach 1956–1989, (93) o rolnictwie ekologicznym, (94) o systemie zarządzania emisjami gazów cieplarnianych i innych substancji, (95) o spółdzielczych kasach oszczędnościowo-kredytowych, (96) o infrastrukturze informacji przestrzennej, (97) o udostępnianiu informacji gospodarczych i wymianie danych gospodarczych, (98) o dowodach osobistych, (99) o ewidencji ludności, (100) o publicznym transporcie zbiorowym, (101) o opiece nad dziećmi w wieku do lat 3, (102) o działalności leczniczej, (103) o systemie informacji w ochronie zdrowia, (104) o Krajowej Radzie Sądownictwa, (105) o kredycie konsumenckim, (106) o wspieraniu rodziny i systemie pieczy zastępczej, (107) o kontroli w administracji rządowej, (108) o bezpieczeństwie osób przebywających na obszarach wodnych, (109) o bezpieczeństwie i ratownictwie w górach i na zorganizowanych terenach narciarskich, (110) o usługach płatniczych, (111) o weteranach działań poza granicami państwa, (112) o przewozie towarów niebezpiecznych, (113) o spłacie niektórych niezaspokojonych należności przedsiębiorców, wynikających z realizacji udzielonych zamówień publicznych, (114) o Państwowej Komisji Badania Wypadków Morskich, (115) o odpadach, (116) o wzajemnej pomocy przy dochodzeniu podatków, należności celnych i innych należności pieniężnych, (117) o systemie powiadamiania ratunkowego, (118) o prawach konsumenta, (119) o charakterystyce energetycznej budynków, (120) Prawo o aktach stanu cywilnego, (121) o komisjach lekarskich podległych ministrowi właściwemu do spraw wewnętrznych, (122) o Karcie Dużej Rodziny, (123) o rybołówstwie morskim, (124) o odnawialnych źródłach energii, (125) o działaczach opozycji antykomunistycznej oraz osobach represjonowanych z powodów politycznych, (126) o systemie handlu uprawnieniami do emisji gazów cieplarnianych, (127) o leczeniu niepłodności, (128) o wspieraniu zrównoważonego rozwoju sektora rybackiego z udziałem Europejskiego Funduszu Morskiego i Rybackiego, (129) o działalności ubezpieczeniowej i reasekuracyjnej, (130) o wykonywaniu Umowy między Rządem Rzeczypospolitej Polskiej a Rządem Stanów Zjednoczonych Ameryki w sprawie poprawy wypełniania międzynarodowych obowiązków podatkowych oraz wdrożenia ustawodawstwa FATCA, (131) o rewitalizacji, (132) o pomocy państwa w wychowywaniu dzieci, (133) o ponownym wykorzystywaniu informacji sektora publicznego, (134) o szczególnych zasadach wykonywania niektórych zadań z zakresu informatyzacji działalności organów Krajowej Administracji Skarbowej, (135) o przeciwdziałaniu zagrożeniom przestępczością na tle seksualnym, (136) o Bankowym Funduszu Gwarancyjnym, systemie gwarantowania depozytów oraz przymusowej restrukturyzacji, (137) o umowie koncesji na roboty budowlane lub usługi, (138) o Krajowej Administracji Skarbowej, (139) Prawo oświatowe, (140) o Prokuratorii Generalnej Rzeczypospolitej Polskiej, (141) o zasadach zarządzania mieniem państwowym, (142) Przepisy wprowadzające ustawę o zasadach zarządzania mieniem państwowym, (143) o wymianie informacji podatkowych z innymi państwami, (144) o systemie monitorowania drogowego i kolejowego przewozu towarów, (145) o zwalczaniu dopingu w sporcie, (146) o biegłych rewidentach, firmach audytorskich oraz nadzorze publicznym, (147) o podstawowej opiece zdrowotnej, (148) o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, (149) o Centralnej Ewidencji i Informacji o Działalności Gospodarczej i Punkcie Informacji dla Przedsiębiorcy, (150) o komornikach sądowych, (151) Prawo o ruchu drogowym, (152) Prawo o szkolnictwie wyższym i nauce.

[162] W ustawie z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (Dz. U. z 2018 r. poz. 2096 oraz z 2019 r. poz. 60) m.in. dodano art. 2a regulujący sposób wykonywania obowiązku, o którym mowa w art. 13 ust. 1 i 2 rozporządzenia. Doprecyzowano, że wykonywanie obowiązku, o którym mowa w art. 13 ust. 1 i 2 rozporządzenia, odbywa się niezależnie od obowiązków organów administracji publicznej przewidzianych w Kodeksie postępowania administracyjnego i nie wpływa na tok i wynik postępowania. Podobnie jak wystąpienie z żądaniem, o którym mowa w art. 18 ust. 1 rozporządzenia nie wpływa na tok i wynik postępowania. Ponadto w art. 54 po § 1 dodano się § 1a ustalający, iż w wezwaniu zawiera się również informacje, o których mowa w art. 13 ust. 1 i 2 rozporządzenia, chyba że wezwany posiada te informacje, a ich zakres lub treść nie uległy zmianie. Organ administracji publicznej przekazuje informacje, o których mowa w art. 13 ust. 1 i 2 rozporządzenia, przy pierwszej czynności skierowanej do strony, chyba że strona posiada te informacje, a ich zakres lub treść nie uległy zmianie. Wreszcie uzupełniono art. 236 regulując, iż w przypadku wszczęcia albo wznowienia postępowania, stwierdzenia nieważności decyzji, jej uchylenia albo zmiany na skutek skargi, o której mowa w art. 233 zdanie drugie, art. 234 pkt 2 lub art. 235, w stosunku do strony i uczestnika postępowania przepisu art. 15 ust. 1 lit. g rozporządzenia nie stosuje się.

TABELA 9 Wybrane zmiany w ustawach sektorowych

1. ustawa Kodeks pracy oraz ustawa o zakładowym funduszu świadczeń socjalnych	
Zakres danych osobowych, jakie pracodawca ma prawo żądać od osoby ubiegającej się o zatrudnienie oraz od pracownika	art.22^{1} KP
Sytuacje oraz warunki, w jakich pracodawca może stosować zgodę na przetwarzanie danych od kandydatów oraz pracowników, a także przetwarzać ich dane biometryczne	art. 22^{1a} i 22^{1b} KP
Sposób, w jaki pracodawca dopuszcza do przetwarzania danych szczególnych kategorii	art. 22^{1b} KP, art. 8 ust. 1b, uZFŚS
Warunki stosowania w zakładzie pracy monitoringu wizyjnego, monitoringu poczty elektronicznej pracowników oraz innych form monitorowania aktywności pracowników	art. 22^{2} i 22^{3} KP
Sposób w jaki pracodawca powinien zbierać i dokumentować dane osobowe osób ubiegających się o udzielenie świadczenia z zakładowego funduszu świadczeń socjalnych, a także jaki jest okres przechowywania takich danych	art. 8 ust. 1a, 1c i 1d uZFŚS
2. ustawa o świadczeniu usług drogą elektroniczną oraz ustawa Prawo telekomunikacyjne	
Wymóg uzyskania zgody adresata na przesłanie treści marketingowych za pośrednictwem narzędzi komunikacji takich jak, np. email, sms, mms oraz połączeń telefonicznych	art. 10 ust. 1–2 uśude, art. 172 ust. 1 Pr. telekom
Konieczność stosowania przepisów ODO do uzyskania zgody marketingowej	art. 5 uśude, art. 174 Pr. telekom
3. ustawa Prawo zamówień publicznych	
Sposób w jaki powinien być spełniony obowiązek informacyjny	art.. 8a ust. 1–7 PZP
Kategorie danych które są wyłączone z zasady jawności protokołu postępowania	art. 96 ust. 3a PZP
Realizowanie prawa do ograniczenia przetwarzania danych z art. 18 RODO w odniesieniu do danych zgromadzonych w protokole postępowania oraz jego załącznikach	art.. 96 ust. 3b PZP
Zasady realizacji prawa dostępu do danych z art. 15 RODO oraz prawa do sprostowania lub uzupełnienia danych z art. 16 RODO w odniesieniu do danych zgromadzonych w protokole postępowania oraz jego załącznikach	art. 97 ust. 1a i 1b PZP
Dokumenty jakie można żądać od wykonawców potwierdzających zatrudnienie na podstawie umowy o pracę osób wykonujących czynności w zakresie realizacji zamówienia	art. 143e PZP

Źródło: M. Szkutnik, *Przepisy o ochronie danych osobowych, czyli nie tylko RODO*, https://blog-daneosobowe.pl/przepisy-o-ochronie-danych-osobowych-czyli-nie-tylko-rodo/, [dostęp: 17.07.2021]

Należy również wyeksponować, iż przepisem art. 161 nowelizacji wprowadzono zmiany w samej ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych, wprowadzając do aktu: art. 5a[163], 6a[164], 11a[165], 101a[166], 108 ust. 2[167], a także zmieniając 57 ust. 1[168].

[163] Art. 5a. 1. Administrator, który otrzymał dane osobowe od podmiotu realizującego zadanie publiczne, nie wykonuje obowiązków, o których mowa w art. 15 ust. 1–3 rozporządzenia 2016/679, w przypadku gdy podmiot przekazujący dane osobowe wystąpił z żądaniem w tym zakresie ze względu na konieczność prawidłowego wykonania zadania publicznego mającego na celu: 1) zapobieganie przestępczości, wykrywanie lub ściganie czynów zabronionych lub wykonywanie kar, w tym ochronę przed zagrożeniami dla bezpieczeństwa publicznego i zapobieganie takim zagrożeniom; 2) ochronę interesów gospodarczych i finansowych państwa obejmującą w szczególności: a) realizację i dochodzenie dochodów z podatków, opłat, niepodatkowych należności budżetowych oraz innych należności, b) wykonywanie egzekucji administracyjnej należności pieniężnych i niepieniężnych oraz wykonywanie zabezpieczenia należności pieniężnych i niepieniężnych, c) przeciwdziałanie wykorzystywaniu działalności banków i instytucji finansowych do celów mających związek z wyłudzeniami skarbowymi, d) ujawnianie i odzyskiwanie mienia zagrożonego przepadkiem w związku z przestępstwami, e) prowadzenie kontroli, w tym kontroli celno-skarbowych. 2. Administrator udziela odpowiedzi na żądanie wniesione na podstawie art. 15 rozporządzenia 2016/679 w sposób, który uniemożliwia ustalenie, że administrator przetwarza dane osobowe otrzymane od podmiotu wykonującego zadanie publiczne.

[164] Art. 6a. 1. Do przetwarzania danych osobowych w ramach wykonywania konstytucyjnych i ustawowych kompetencji Prezydenta Rzeczypospolitej Polskiej, w zakresie nieobjętym bezpieczeństwem narodowym, stosuje się odpowiednio przepisy art. 4–7, art. 11, art. 12, art. 16, art. 17, art. 24 ust. 1 i 2, art. 25 ust. 1 i 2, art. 28–30, art. 32, art. 34, art. 35, art. 37–39 i art. 86 rozporządzenia 2016/679 oraz przepisy art. 6 i art. 11 ustawy. 2. Przetwarzanie danych, o których mowa w art. 9 i art. 10 rozporządzenia 2016/679, następuje w zakresie niezbędnym do realizacji konstytucyjnych i ustawowych kompetencji Prezydenta Rzeczypospolitej Polskiej, jeżeli prawa lub wolności osoby, której dane dotyczą, nie są nadrzędne w stosunku do realizacji zadań wynikających z tych kompetencji.

[165] Art. 11a. 1. Podmiot, który wyznaczył inspektora, może wyznaczyć osobę zastępującą inspektora w czasie jego nieobecności, z uwzględnieniem kryteriów, o których mowa w art. 37 ust. 5 i 6 rozporządzenia 2016/679. 2. W związku z wykonywaniem obowiązków inspektora w czasie jego nieobecności do osoby go zastępującej stosuje się odpowiednio przepisy dotyczące inspektora. Podmiot, który wyznaczył osobę zastępującą inspektora, zawiadamia Prezesa Urzędu o jej wyznaczeniu w trybie art. 10 oraz udostępnia jej dane zgodnie z art. 11.

[166] Art. 101a. 1. W związku z toczącym się postępowaniem w sprawie nałożenia administracyjnej kary pieniężnej, podmiot, o którym mowa w art. 101, jest obowiązany do dostarczenia Prezesowi Urzędu, na każde jego żądanie, w terminie 30 dni od dnia otrzymania żądania, danych niezbędnych do określenia podstawy wymiaru administracyjnej kary pieniężnej. 2. W przypadku niedostarczenia danych przez podmiot, o którym mowa w art. 101, lub gdy dostarczone przez ten podmiot dane uniemożliwiają ustalenie podstawy wymiaru administracyjnej kary pieniężnej, Prezes Urzędu ustala podstawę wymiaru administracyjnej kary pieniężnej w sposób szacunkowy uwzględniając wielkość podmiotu, specyfikę prowadzonej przez niego działalności lub ogólnie dostępne dane finansowe dotyczące podmiotu.

[167] Tej samej karze podlega kto, w związku z toczącym się postępowaniem w sprawie nałożenia administracyjnej kary pieniężnej, nie dostarcza danych niezbędnych do określenia podstawy wymiaru administracyjnej kary pieniężnej lub dostarcza dane, które uniemożliwiają ustalenie podstawy wymiaru administracyjnej kary pieniężnej.

[168] Administrator może wystąpić do Prezesa Urzędu z wnioskiem o przeprowadzenie uprzednich konsultacji, o których mowa w art. 36 rozporządzenia 2016/679.

Przetwarzanie danych osobowych przez instytucje i organy UE

Zgodnie z art. 8 Karty Praw Podstawowych UE każdy ma prawo do ochrony danych osobowych[169]. Prawo to rozwinięto w art. 16 Traktatu o Funkcjonowaniu Unii Europejskiej[170]. Prawo to gwarantuje również art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności oraz szereg aktów prawa międzynarodowego[171]. Zasady te odnoszą się nie tylko na zewnątrz ale także do wewnątrz struktur organizacyjnych Wspólnoty. Kluczowym aktem prawnym regulującym zasady przetwarzania przez instytucje i organy Unii Europejskiej, a także przez jej jednostki organizacyjne, danych osobowych osób fizycznych, które znajdują się w ich posiadaniu, jest 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[172], jak również komplementarna wobec niego decyzja Komisji (UE) 2020/969 z dnia 3 lipca 2020 r. określająca przepisy wykonawcze dotyczące inspektora ochrony danych, ograniczeń praw osób, których dane dotyczą, i stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725[173]. Akty te uchyliły dotychczas obowiązujące rozporządzenie (WE) nr 45/2001[174], decyzję Komisji 2008/597/WE[175] oraz decyzję nr 1247/2002/WE dotyczącą Europejskiego Inspektora Ochrony Danych (EIOD)[176]. W zastosowaniu pozostała 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[177].

W przepisach zapewnia się te same restrykcyjne normy, które określono w RODO, wobec procesów przetwarzania danych osobowych przez instytucje, organy i jednostki organizacyjne UE, co ma narzucić ten sam standard systemu GDPR i pozwolić zagwarantować podstawowe prawa i wolności osób fizycznych, w szczególności ich prawo do ochrony danych osobowych i prawo do prywatności[178]. W szczególności rozporządzenie 2018/1725 dostosowuje przepisy obowiązujące instytucje, organy i jednostki organizacyjne UE do przepisów RODO oraz dyrektywy (UE) 2016/680, czyli dyrektywy w sprawie ochrony osób fizycznych w związku

[169] Karta praw podstawowych Unii Europejskiej (Dz.Urz. UE C 326 z 26.10.2012 r., s. 391–407).
[170] Traktat o Unii Europejskiej i Traktat o funkcjonowaniu Unii Europejskiej – wersja skonsolidowana (Dz. Urz. C 326 z 26.10.2012 r., s. 1).
[171] Międzynarodowe Standardy Ochrony Danych Osobowych i Prywatności, Rezolucja Madrycka, 5.11.2009.
[172] (Tekst mający znaczenie dla EOG) (Dz. Urz. UE L 295 z 21.11.2018r., s. 39–98). Rozporządzenie weszło w życie 11 grudnia 2018 roku, z wyjątkiem przetwarzania danych osobowych przez Eurojust, w którym to przypadku zastosowanie aktywizowało się 12 grudnia 2019 roku.
[173] Dz.U. L 213 z 6.7.2020 r., s. 12–22.
[174] Rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych (Dz.Urz. UE L 8 z 12.1.2001 r., s. 1–22).
[175] Decyzja nr 2008/597/WE Komisji z dnia 3 czerwca 2008 r. w sprawie przyjęcia przepisów wykonawczych w zakresie inspektora ochrony danych zgodnie z art. 24 ust. 8 rozporządzenia (WE) nr 45/2001 o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych (Dz.Urz. UE L 193 z 22.7.2008 r., s. 7–11).
[176] Decyzja nr 1247/2002/WE Parlamentu Europejskiego, Rady i Komisji z dnia 1 lipca 2002 r. w sprawie regulaminu i ogólnych warunków regulujących wykonywanie obowiązków przez Europejskiego Pełnomocnika ds. Ochrony Danych (Dz.Urz. UE L 183 z 12.7.2002 r., s. 1–2).
[177] Dz.U. UE L 119 z 4.5.2016 r., s. 89–131.
[178] Zob. M. Safjan, *Prawo do prywatności i ochrona danych osobowych w społeczeństwie informatycznym*, Państwo i Prawo 2002, nr 6, s. 3–12; Por. A. Mednis, *Prawo do prywatności a interes publiczny,* Wolters Kluwer, Warszawa 2006.

z przetwarzaniem danych osobowych do celów zapobiegania przestępczości, które mają zastosowanie od maja 2018 roku[179]. Oznacza to, że zasady oraz instytucje ochrony danych osobowych panujące w ramach reżimu RODO, tutaj mają swoje lustrzane odzwierciedlenie. I tak, dane osobowe muszą być: (a) przetwarzane zgodnie z prawem, w sposób rzetelny i przejrzysty, (b) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach, (c) adekwatne, stosowne i ograniczone do tego, co niezbędne, (d) prawidłowe i w razie potrzeby uaktualniane, (e) przechowywane w sposób umożliwiający identyfikację osób, których dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne, (f) przetwarzane w sposób zapewniający odpowiednią poufność[180]. Zgodnie z rozporządzeniem osoby, których dane dotyczą mają prawo do:

- wycofania w dowolnym momencie wyrażonej zgody, przy czym wycofanie zgody musi być równie łatwe jak jej wyrażenie,
- informacji, czy ich dane osobowe są przetwarzane, czy też nie, a także dostępu do tych danych,
- sprostowania wszelkich nieprawidłowych danych osobowych,
- usunięcia danych osobowych lub ograniczenia ich przetwarzania, o ile spełnione są określone warunki,
- otrzymania swoich danych osobowych w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego,
- sprzeciwu, z przyczyn związanych z ich szczególną sytuacją, wobec wykorzystywania ich danych osobowych z uwagi na względy interesu publicznego,
- niepodlegania decyzji wywołującej dla nich skutki prawne, która opiera się wyłącznie na przetwarzaniu zautomatyzowanym,
- złożenia skargi do EIOD, jeżeli uważają, że ich dane osobowe są przetwarzane w sposób sprzeczny z przepisami rozporządzenia,
- otrzymania odszkodowania za każdą szkodę majątkową lub niemajątkową wyrządzoną działaniem instytucji, organu lub jednostki organizacyjnej UE,
- umocowania organizacji trzeciego sektora do wniesienia skargi do EIOD[181].

Administratorem danych jest instytucja lub organ Unii (jednostka organizacyjna Unii ustanowiona TUE, TFUE lub Traktatem Euratom, lub na ich podstawie) lub dyrekcja generalna

[179] Przepisy rozporządzenia 2018/1725 mają także zastosowanie do organów i jednostek organizacyjnych UE, które przetwarzają operacyjne dane osobowe w celach związanych ze ściganiem przestępstw (np. Eurojust). Zostały one uwzględnione w odrębnym rozdziale. Ponadto w aktach założycielskich tych organów i jednostek organizacyjnych przewidziano możliwość ustanowienia bardziej szczegółowych przepisów w celu uwzględnienia ich specyfiki. Z zakresu stosowania rozporządzenia czasowo wyłączono Europol i Prokuraturę Europejską (do kwietnia 2022 roku Komisja ma dokonać przeglądu ram prawnych regulujących przetwarzanie operacyjnych danych osobowych przez organy i jednostki organizacyjne UE w celach związanych ze ściganiem przestępstw). Zob. *Ochrona osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne UE*, https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=LEGISSUM:4374552, [dostęp: 20.01.2021].

[180] Dane osobowe mogą być przesyłane do odbiorcy w UE, który nie jest instytucją, organem lub jednostką organizacyjną UE, jedynie pod warunkiem zastosowania dodatkowych zabezpieczeń (poza UE jedynie na ściśle określonych warunkach). Art. 4 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 oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE (Dz. Urz. UE L 295 z 21.11.2018 r., s. 39–98).

[181] Rozdział III 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 oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE (Dz. Urz. UE L 295 z 21.11.2018 r., s. 39–98).

lub jakakolwiek inna jednostka organizacyjna, która samodzielnie lub łącznie z innymi określa cele i sposoby przetwarzania danych osobowych (jeżeli cele i sposoby takiego przetwarzania danych są określone w szczególnym akcie Unii, prawo Unii może przewidywać wyznaczenie administratora lub określać szczególne kryteria jego wyznaczania)[182]. Administrator odpowiada za przestrzeganie wszystkich zasad dotyczących przetwarzania danych i musi być w stanie wykazać fakt ich przestrzegania, w szczególności administratorzy:

- informują osoby fizyczne, przy użyciu prostego języka oraz z podaniem informacji faktycznych takich jak dane kontaktowe i cele przetwarzania, o fakcie zbierania danych osobowych,
- odpowiadają na wszystkie wnioski składane przez osobę, której dane dotyczą, na przykład w przedmiocie dostępu do danych osobowych, ich sprostowania lub poprawienia, możliwie jak najszybciej i nie później niż w terminie jednego miesiąca,
- stosują odpowiednie środki techniczne i organizacyjne, w tym pseudonimizacji, w celu zapewnienia, aby przetwarzanie odbywało się w sposób zgodny z rozporządzeniem,
- korzystają wyłącznie z usług tych podmiotów przetwarzających dane, które spełniają wymogi UE,
- prowadzą szczegółowy wykaz czynności przetwarzania, za które odpowiadają,
- współpracują z Europejskim Inspektorem Ochrony Danych (EOID),
- możliwie jak najszybciej informują EIOD i zainteresowaną osobę fizyczną o każdym przypadku naruszenia danych osobowych,
- dokonują oceny wpływu nowych technologii przetwarzania na ochronę danych osobowych,
- zapewniają poufność i bezpieczeństwo swoich sieci łączności elektronicznej,
- informują EIOD o opracowywanych środkach administracyjnych lub przepisach wewnętrznych dotyczących przetwarzania danych osobowych[183].

Administratorzy powołują również – na okres od trzech do pięciu lat – Inspektora Ochrony Danych, który m.in. udziela niezależnych porad na temat przetwarzania danych osobowych, zapewnia by osoby, których dane dotyczą, były informowane o swoich prawach i obowiązkach wynikających z rozporządzenia, czy monitoruje przestrzeganie przepisów w dziedzinie ochrony danych[184]. Decyzje sektorowe ustalają zasady określania, kto w danym organie jest odpowiedzialny za operacje przetwarzania przeprowadzane w imieniu organu. W związku z tym wprowadza się pojęcie administratora delegowanego[185], aby dokładnie wskazać obowiązki, w szczególności

[182] Art. 3 pkt 8–10 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 oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE (Dz. Urz. UE L 295 z 21.11.2018 r., s. 39–98).

[183] Zob. *Ochrona osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne UE*, https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=LEGISSUM:4374552, [dostęp: 20.01.2021].

[184] Art. 45 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 oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE (Dz. Urz. UE L 295 z 21.11.2018 r., s. 39–98).

[185] Administratorzy delegowani działają w imieniu Komisji jako administratorzy do celów stosowania rozporządzenia (UE) 2018/1725. Administrator delegowany: (a) wyznacza administratora odpowiedzialnego za operację przetwarzania, który ma wspierać administratora delegowanego w zapewnieniu przestrzegania przepisów rozporządzenia (UE) 2018/1725, (b) zapewnia istnienie wewnętrznych porozumień z innymi dyrekcjami generalnymi lub służbami, jeżeli administrator delegowany prowadzi operacje przetwarzania wspólnie z tymi dyrekcjami generalnymi lub służbami lub jeżeli te dyrekcje generalne lub służby prowadzą część operacji przetwarzania, za które odpowiada administrator delegowany. Zob. Art. 8 decyzji Komisji (UE) 2020/969 z dnia 3 lipca 2020 r. określająca przepisy wykonawcze dotyczące inspektora ochrony danych, ograniczeń praw osób, których dane dotyczą, i stosowania rozporządzenia

w odniesieniu do indywidualnych decyzji dotyczących praw osób, których dane dotyczą. Ponadto wprowadza się pojęcie administratora odpowiedzialnego za operację przetwarzania[186], który – na odpowiedzialność administratora delegowanego – zostaje wyznaczony do zapewnienia zgodności z przepisami w praktyce oraz do rozpatrywania wniosków osób, których dane dotyczą, w odniesieniu do operacji przetwarzania. W niektórych przypadkach kilka służb danego organu (np. Komisji Europejskiej) może wspólnie przeprowadzać operację przetwarzania w celu wypełnienia swojej misji. W takich przypadkach powinny one zapewnić istnienie porozumień wewnętrznych w celu przejrzystego określenia swoich odpowiednich obowiązków wynikających z rozporządzenia 2018/1725. Aby ułatwić wykonywanie obowiązków administratorów delegowanych, każda służba Komisji powinna wyznaczyć koordynatora ds. ochrony danych[187].

Na mocy rozporządzenia utworzono także urząd Europejskiego Inspektora Ochrony Danych (EIOD), który z kolei działa na mocy regulaminu wewnętrznego przyjętego decyzją z dnia 15 maja 2020 roku[188]. Jest on powoływany na pięcioletnią kadencję, która może być odnowiona jeden raz. Siedziba Europejskiego Inspektora Ochrony Danych mieści się w Brukseli, zaś osoba zajmująca to stanowisko – poza tym że działa w sposób w pełni niezależny – m.in. (a) podlega obowiązkowi zachowania tajemnicy służbowej w odniesieniu do wszelkich informacji poufnych, (b) monitoruje stosowanie przepisów rozporządzenia przez instytucje, organy i jednostki organizacyjne UE, (c) upowszechnia w społeczeństwie wiedzę o przetwarzaniu danych osobowych i rozumienie tego zjawiska, (d) rozpatruje skargi i prowadzi postępowania, (e) udziela administratorom danych ostrzeżeń i nakłada na nich kary, (f) przekazuje sprawy do Trybunału Sprawiedliwości, który rozstrzyga wszelkie spory dotyczące rozporządzenia, (g) przedkłada roczne sprawozdanie Parlamentowi Europejskiemu, Radzie i Komisji Europejskiej, (h) współpracuje z krajowymi organami nadzorczymi w dziedzinie ochrony danych[189].

Parlamentu Europejskiego i Rady (UE) 2018/1725 oraz uchylająca decyzję Komisji 2008/597/WE (Dz.U. L 213 z 6.7.2020, s. 12–22).

[186] Administrator odpowiedzialny za operację przetwarzania: (a) przyjmuje i rozpatruje wszystkie wnioski osób, których dane dotyczą, (b) powiadamia Europejskiego Inspektora Ochrony Danych (EIOD) o ewentualnym naruszeniu ochrony danych osobowych, (c) w przypadku naruszenia ochrony danych osobowych, informuje o tym koordynatora ds. ochrony danych i inspektora ochrony danych oraz – w stosowanych przypadkach – osobę, której dane dotyczą, (d) zapewnia, by koordynator ds. ochrony danych był informowany o wszelkich kwestiach związanych z ochroną danych, w szczególności o wnioskach osób, których dane dotyczą, (e) wykonuje wszelkie inne zadania wchodzące w zakres niniejszej decyzji na wniosek administratora delegowanego. Zob. Art. 8 decyzji Komisji (UE) 2020/969 z dnia 3 lipca 2020 r. określająca przepisy wykonawcze dotyczące inspektora ochrony danych, ograniczeń praw osób, których dane dotyczą, i stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 oraz uchylająca decyzję Komisji 2008/597/WE (Dz.U. L 213 z 6.7.2020, s. 12–22).

[187] Koordynatorów ds. ochrony danych wybiera się na podstawie ich wiedzy i doświadczenia w zakresie funkcjonowania danej dyrekcji generalnej lub służby, ich motywacji do sprawowania tej funkcji, kompetencji związanych z ochroną danych, zrozumienia zasad systemów informacyjnych i umiejętności komunikacyjnych. Koordynator ds. ochrony danych pełni rolę punktu kontaktowego między administratorem delegowanym, administratorem odpowiedzialnym za operację przetwarzania i podmiotem przetwarzającym dane a inspektorem ochrony danych. Koordynator ds. ochrony danych prowadzi zapisy i przekazuje zanonimizowane dane statystyczne dotyczące wniosków osób, których dane dotyczą, do dyrekcji generalnej, służby lub gabinetu, określając liczbę wniosków i liczbę wniosków odrzuconych w całości lub w części. Inspektor ochrony danych określa kategorie wniosków, w odniesieniu do których należy gromadzić dane statystyczne. Inspektor ochrony danych może określić, jakie dalsze szczegółowe informacje należy przedstawić. Koordynator ds. ochrony danych przechowuje zanonimizowane dane statystyczne dotyczące naruszeń ochrony danych osobowych, którymi zarządza dana dyrekcja generalna, służba lub gabinet; dane te określają łączną liczbę przypadków naruszenia ochrony danych osobowych, liczbę przypadków naruszenia ochrony danych osobowych, o których to przypadkach powiadomiono EIOD, oraz liczbę przypadków naruszenia ochrony danych osobowych zgłoszonych osobom, których dane dotyczą. Koordynator ds. ochrony danych upowszechnia wiedzę o kwestiach związanych z ochroną danych w swojej dyrekcji generalnej lub służbie, doradza administratorom delegowanym i administratorom odpowiedzialnym za operacje przetwarzania w wypełnianiu ich obowiązków i wspiera ich w wypełnianiu tych obowiązków, w szczególności w odniesieniu do: (a) wdrażania ogólnych zasad rozporządzenia 2018/1725, (b) dokumentowania operacji przetwarzania, (c) przekazywania inspektorowi ochrony danych zapisów dotyczących operacji przetwarzania, (d) przygotowania oświadczeń o ochronie prywatności. Art. 7 decyzji Komisji (UE) 2020/969 z dnia 3 lipca 2020 r. określająca przepisy wykonawcze dotyczące inspektora ochrony danych, ograniczeń praw osób, których dane dotyczą, i stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 oraz uchylająca decyzję Komisji 2008/597/WE (Dz.U. L 213 z 6.7.2020, s. 12–22).

[188] W regulaminie wewnętrznym EIOD określono szczegółowo m.in.: (a) misję, wytyczne i organizację EIOD, (b) sposób monitorowania i zapewnienia stosowania rozporządzenia, (c) procedury dotyczące konsultacji w sprawie aktów ustawodawczych, monitorowania technologii, projektów badawczych i postępowań sądowych, oraz (d) procedury współpracy z krajowymi organami nadzorczymi i współpracy międzynarodowej. Zob. Decyzja Europejskiego Inspektora Ochrony Danych z dnia 15 maja 2020 r. w sprawie przyjęcia regulaminu wewnętrznego EIOD (Dz. Urz. UE L 204 z 26.6.2020, s. 49–59).

[189] Zob. Rozdział VI 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 oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE (Dz. Urz. UE L 295 z 21.11.2018 r., s. 39–98).

Katalog najważniejszych zmian systemu ochrony danych osobowych

Unijny model ochrony danych to kluczowy zestaw reguł kształtujących obowiązki administratorów danych i uprawnienia podmiotów danych, które nadal pozostają swoistym wzorem dla innych części świata, chociażby z uwagi na europejski rodowód tej dziedziny prawa. Unijny porządek ukształtowany rozporządzeniem 2016/679 bezwzględnie podtrzymał kontinuum m.in. w zakresie przetwarzania danych wyłącznie na określonej podstawie prawnej (np. zgody podmiotu danych, lub w ramach uprawnienia albo obowiązku określonego w konkretnym przepisie prawa), zapewnienia podmiotowi danych informacji o ich przetwarzaniu oraz prawa dostępu do danych, poprawiania ich i sprzeciwu wobec ich przetwarzania, wymogu analizy otoczenia towarzyszącego przetwarzaniu danych, czy obowiązku zabezpieczenia danych m.in. przed nieuprawnionym dostępem lub modyfikacją, wreszcie statusu Inspektora Ochrony Danych czy stosowania zasad: (1) celowości (*purpose limitation)*, (2) jakości danych (*accuracy)*, (3) adekwatności (*data minimisation, adequacy)*, (4) ograniczenia czasowego (*storage minimisation)*, czy (5) adekwatności ochrony przy międzynarodowych transferach danych – jednocześnie jednak wprowadzając katalog nowych wymogów i instytucji.

Nowe przepisy wprowadziły szereg nieznanych wcześniej obowiązków dla przedsiębiorców – administratorów danych, w tym m.in.: (a) obowiązek powołania Inspektora Ochrony Danych, (b) prowadzenie rejestrów czynności przetwarzania danych, (c) wykonywanie procedur oceny ryzyk, (d) zmianę klauzul informacyjnych w stosunku do klientów B2B, B2C, procesów rekrutacyjnych, sprawozdawczości finansowej i spraw kadrowych, (e) realizację prawa do przenoszenia danych, czy prawa do bycia zapomnianym i profilowania[190].

[190] Analizując nowe rozporządzenie należy zauważyć, iż przepisy zakładają zmianę aksjologiczną w podejściu do zarządzania danymi osobowymi, wyrażającą się m.in.: (a) rozszerzeniem zakresu przedmiotowego definiowanych terminów, (b) wprowadzeniem domniemania zwięzłej, przejrzystej, łatwo dostępnej i zrozumiałej formy kierowania informacji, w szczególności do dzieci, (c) ustanawiają kategorię profilowania, współadministrowania, rejestrowania czynności przetwarzania, (d) zmieniają częściowo zasady przekazywania informacji pozyskanych w sposób inny niż od osoby, której dane dotyczą, (e) ustanawiają międzynarodową współpracę na rzecz ochrony danych osobowych, (f) porządkują podstawy prawne funkcjonowania organów nadzorczych, (g) ustanawiają Europejską Radę Ochrony Danych. Zmiany dotyczą wielu aspektów działalności firm i jednostek organizacyjnych. Należy przy tym pamiętać, że Administratorem Danych – w rozumieniu przepisów – jest w praktyce każdy przedsiębiorca. Norma prawna uwydatnia natomiast rolę Inspektora Ochrony Danych. Administrator i podmiot przetwarzający wyznaczają Inspektora Ochrony Danych, w każdym przypadku, w którym: (1) przetwarzania dokonuje organ lub podmiot publiczny; (2) przetwarzania dokonuje osoba prawna i dotyczy ono ponad 5000 podmiotów danych rocznie w dowolnym okresie kolejnych 12 miesięcy; (3) główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania podmiotów danych; (4) główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu szczególnych kategorii danych dotyczących lokalizacji lub danych dotyczących dzieci lub pracowników w wielkoskalowych zbiorach danych. Istotną zmianą jest także możliwość wyznaczenia w ramach grupy przedsiębiorstw głównego odpowiedzialnego inspektora ochrony danych, pod warunkiem zapewnienia łatwego kontaktu z inspektorem ochrony danych z każdej siedziby. Jeśli administrator lub podmiot przetwarzający są organem lub podmiotem publicznym, inspektor ochrony danych może być wyznaczony dla szeregu jego jednostek organizacyjnych, z uwzględnieniem struktury organizacyjnej organu lub podmiotu publicznego. Administrator lub podmiot przetwarzający wyznaczają inspektora ochrony danych na podstawie jego kwalifikacji zawodowych oraz w szczególności jego wiedzy specjalistycznej z zakresu prawa ochrony danych, praktyki i zdolności do wykonywania zadań określonych w rozporządzeniu. Niezbędny poziom wiedzy specjalistycznej ustala się w szczególności zgodnie z prowadzonym przetwarzaniem danych oraz ochroną wymaganą dla danych osobowych przetwarzanych przez administratora lub podmiot przetwarzający. Nadto, administrator lub podmiot przetwarzający informują organ nadzorczy oraz opinię publiczną o imieniu i nazwisku oraz danych kontaktowych inspektora ochrony danych. Wśród

Przy całej kompleksowości reformy systemu danych osobowych, należy zauważyć, że nie uległy zmianie konieczność spełniania wymogów w zakresie:

- wdrożenia systemu bezpieczeństwa danych osobowych, w tym posiadania prawidłowo opracowanej dokumentacji, w tym: (a) Polityki Ochrony Danych Osobowych, (b) Instrukcji Zarządzania Systemem Informatycznym Służącym do Przetwarzania Danych Osobowych (z zastrzeżeniem, że samo rozporządzenie – z pewnymi wyjątkami – nie wprowadziło obowiązku fizycznego posiadania takiej dokumentacji);
- przeprowadzenia szkoleń dla pracowników przetwarzających dane osobowe;
- audytu i ewaluacji systemu bezpieczeństwa danych osobowych,
- kontroli prawidłowości przestrzegania norm i zasad.

Nowe przepisy wprowadziły natomiast rewolucję w zakresie kar administracyjnych za niedopełnienie obowiązków wynikających z przepisów. Ich wysokość kształtuje się w zależności od kategorii naruszeń, wagi, czasu trwania, liczby poszkodowanych osób, umyślności bądź nieumyślności naruszenia, kategorii danych osobowych, których dotyczyło naruszenie i wynosi: (1) do 10 000 000 euro, a w przypadku przedsiębiorstwa – w wysokości do 2 % jego całkowitego rocznego obrotu z poprzedniego roku; (2) przypadku cięższych naruszeń do 20 000 000 euro, a w przypadku przedsiębiorstwa – w wysokości do 4 % jego całkowitego rocznego obrotu z poprzedniego roku obrotowego.

Odnosząc się bardziej szczegółowo do zmian wprowadzonych rozporządzeniem 2016/679 można wyróżnić katalog przestrzeni materialno-prawnych stanowiących *novum*, względnie istotną zmianę w europejskim systemie ochrony danych osobowych, w tym przy zastosowaniu systematyki jak następuje:

1) **dyferencjacja obowiązków prawnych dopasowanych do rodzaju administratora danych** – wprowadzenie rozróżnienia na małe oraz większe jednostki organizacyjne z szeregiem konsekwencji prawnych, z tego tytułu płynących;
2) **ułatwienie składania skarg do organów nadzorczych** – w tym zapewnienie możliwości złożenia skargi bezpłatnie oraz do dowolnego organu nadzorczego w Unii;
3) **przyjęcie domyślnej prywatność od podstaw (*privacy by design i privacy by default*)** – nałożenie na administratorów danych nowych obowiązków w zakresie podjęcia działań określanych jako obowiązek uwzględniania ochrony danych w fazie projektowania (*privacy by design*), jak i już w fazie samego przetwarzania danych osobowych (*privacy by default*);
4) **powołanie funkcji Inspektora Ochrony Danych przy jednoczesnej anulacji funkcji Administratora Bezpieczeństwa Informacji** – uchylenie pozycji ABI (Administrator

wskazanych przepisów szczególne zaciekawienie budzi sposób interpretacji trzeciej sytuacji, w której powołanie inspektora będzie obligatoryjne, tj. gdy główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania podmiotów danych. Zob. 37 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 (Dz. Urz. UE L 119 z dn. 4.05.2016, s. 1–88).

Bezpieczeństwa Informacji) przy jednoczesnym utworzeniu stanowiska IOD (Inspektor Ochrony Danych), którego powołanie, w przeciwieństwie do ABI, jest co do zasady obowiązkowe lub zalecane (w przypadku małych i mikro przedsiębiorców), z tym zastrzeżeniem, że grupa przedsiębiorstw po pierwsze może powołać jednego Inspektora Ochrony Danych w ramach jednej grupy kapitałowej, po drugie funkcja IOD może być *outsourcowana*, po trzecie na Inspektora Ochrony Danych nałożono szereg dodatkowych obowiązków (w relacji do obowiązków ABI), po czwarte IOD uzyskał odmienną rolę i pozycję w organizacji niż wcześniejszy ABI;

5) **przyjęcie koncepcji *Risk Based Approach*** – która zakłada, że im większe jest ryzyko związane z przetwarzaniem danych osobowych, tym większy powinien być zakres obowiązków ciążących na administratorze danych, w szczególności w kontekście zastosowanych rozwiązań technologicznych (jak np. Big Data czy chmura obliczeniowa – *cloud computing*), czy samej treści gromadzonych informacji (im zakres przetwarzanych danych jest szerszy bądź znajdują się w nim dane osobowe wrażliwe, tym poziom zabezpieczenia danych powinien być wyższy);
6) **likwidacja obowiązku kategoryzowania zbiorów danych i ich rejestrowania w organie nadzorczym** – pod reżimem prawnym ustawy o ochronie danych osobowych z 1997 roku jednym z ustawowych zadań Generalnego Inspektora Ochrony Danych Osobowych było prowadzenie jawnego rejestru zbiorów danych osobowych, przy czym koncepcja budowania bezpieczeństwa na podstawie wyodrębnionych zbiorów danych była fundamentem systemu do 2018 roku, bez którego nie można było mówić o jakiejkolwiek ochronie danych, bowiem nie było możliwe stworzenie dokumentacji bezpieczeństwa, a w konsekwencji wdrożenie jej postanowień, czy przeprowadzenie audytów, przy czym RODO choć zrezygnowało z konieczności zestawiania i rejestrowania zbiorów danych to w praktyce jednak zastąpiło ten obowiązek na rzecz prowadzenia rejestrów czynności przetwarzania danych osobowych (które to jednak nie mają charakteru publicznego, podlegającego obowiązkowi notyfikacji, czy rejestracji w organie administracji publicznej);
7) **nałożenie konieczności dokonywania oceny skutków przetwarzania (*privacy impact assessment*)** – już podczas projektowania systemu ochrony danych osobowych należy wdrażać takie środki, by od samego początku chronić przetwarzane dane oraz prywatność osób, których dane dotyczą – co przenosi ciężar odpowiedzialności za niezgodne z prawem przetwarzanie danych osobowych na administratorów, przy czym rozwinięciem praktycznych aspektów ochrony prywatności w fazie projektowania jest obowiązek dokonywania oceny ryzyka i skutków wpływu na prywatność oraz poziom ochrony danych (*impact assessment*), a do jej przeprowadzania administrator danych lub podmiot przetwarzający są zobowiązani wówczas, gdy operacje przetwarzania stwarzają szczególne ryzyko dla praw i wolności podmiotów danych z racji swego charakteru,

zakresu lub celów (żeby przynosiła oczekiwane rezultaty powinna być przeprowadzana zanim jakieś urządzenia czy systemy zostaną wprowadzone do użycia);

8) **wprowadzenie możliwości przetwarzania danych osobowych wspólnie przez grupy kapitałowe, grupy przedsiębiorców w ramach współadministracji danymi osobowymi** – kilka podmiotów (grupa przedsiębiorstw oznaczająca przedsiębiorstwo sprawujące kontrolę oraz przedsiębiorstwa przez nie kontrolowane) może jednocześnie administrować tymi samymi danymi, z zastrzeżeniem wszystkich konsekwencji wynikających z prawa (np. obowiązek informacyjny wobec osób, których dane dotyczą, ze wskazaniem kto i za co odpowiada);
9) **wdrożenie rejestru czynności związanych z przetwarzaniem danych** – administratorzy danych oraz podmioty przetwarzające muszą wdrożyć budować system ochrony danych w oparciu o identyfikację czynności i celów przetwarzania oraz wdrożenie odpowiednich środków technicznych i organizacyjnych, które zapewnią prowadzenie rejestru czynności przetwarzania danych (w przypadku administratora), bądź rejestru kategorii czynności przetwarzania (w przypadku procesora);
10) **raportowanie naruszenia bezpieczeństwa danych do administracyjnego organu nadzorczego** – administrator danych oraz procesor są zobowiązani do zgłoszenia naruszenia ochrony danych osobowych, spełniającego wymóg uzasadnionego wyjaśnienia, bez zbędnej zwłoki, a jeżeli jest to wykonalne, nie później niż w czasie 72h po stwierdzeniu naruszenia;
11) **poszerzenie katalogu danych wrażliwych (sensytywnych)** – w szczególności o dane biometryczne [pełen katalog danych wrażliwych pod rządami RODO wygląda jak następuje; dane: (a) ujawniające pochodzenie rasowe lub etniczne, (b) ujawniające poglądy polityczne, (c) ujawniające przekonania religijne lub światopoglądowe, (d) ujawniające przynależność do związków zawodowych, (e) genetyczne, (f) biometryczne (wykorzystywane w celu jednoznacznego zidentyfikowania osoby fizycznej), (g) dotyczące zdrowia, (h) dotyczące seksualności lub orientacji seksualnej];
12) **modyfikacja konstrukcji zgody na przetwarzanie danych** – zgodnie z nową definicją 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 przyzwolenie na przetwarzanie dotyczących jej danych osobowych;
13) **wprowadzenie „pseudonimizacji" danych osobowych** – przetwarzanie danych osobowych musi się odbywać w taki sposób, by nie można ich było przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, o ile takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;

14) **zwiększenie kontroli nad danymi osobowymi podmiotów, których dane są przetwarzane** – w szczególności poprzez wprowadzenie nowego uprawnienia podmiotów danych: prawa żądania usunięcia danych (prawo do bycia zapomnianym);
15) **wprowadzenie kontroli na profilowaniem** – osoba, której dane dotyczą ma prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na profilowaniu danymi, tj. zautomatyzowanym przetwarzaniu, wywołującym skutki prawne lub w podobny sposób istotnie na nią wpływającym, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;
16) **rozszerzenie obowiązku informacyjnego w trakcie zbierania informacji o charakterze prywatnym** – spełnienie obowiązku informacyjnego implikowało konieczność wprowadzenia znacznie większej ilości klauzul informacyjnych podczas zbierania danych, przy czym katalog informacyjny został poszerzony m.in. o dane dotyczące: Inspektora Ochrony Danych (nazwa, dane kontaktowe) jeżeli został powołany, podstawę prawną przetwarzania, prawnie uzasadnionego interesu administratora, jeżeli na tej podstawie odbywa się przetwarzanie, zamiar przekazywania danych do państwa trzeciego, okresu przez który dane osobowe będą przechowywane bądź kryteria ustalania tego okresu, profilowaniu, prawa wniesienia skargi do organu nadzorczego, a w przypadku istnienia obowiązku podania danych osobowych, wskazanie ewentualnych konsekwencji niepodania danych, prawach osoby, której dane dotyczą tj. prawie do: usunięcia danych, ograniczenia przetwarzania, prawie przenoszenia danych, prawie do cofnięcia zgody;
17) **wprowadzenie zasad dotyczących przetwarzania danych dzieci** – zgodę na przetwarzanie danych osobowych może wyrazić osoba, która ukończyła 16 lat, w przeciwnym wypadku zgodę musi wyrazić w imieniu dziecka lub zaaprobować osoba sprawująca władzę rodzicielską lub opiekę (na przetwarzającym dane spoczywa obowiązek dokonania weryfikacji wieku użytkownika oraz tego czy opiekun prawny dziecka udzielił zgody lub ją zaaprobował);
18) **doprecyzowanie zasad dotyczących transferu danych do państw trzecich** – przy określeniu warunków dopuszczalności przekazywania danych do państwa trzeciego przyjęto zasadę, że eksporter danych (administrator lub procesor) powinien oprzeć transfer na jednym z trzech podstawowych mechanizmów transferowych: (a) decyzji Komisji Europejskiej stwierdzającej odpowiedniość ochrony w państwie trzecim, (b) odpowiednich gwarancji ochrony danych osobowych, (c) uwzględnieniu wyjątków określonych w art. 44 rozporządzenia;
19) **wzmocnienie współpracy pomiędzy organami nadzoru państw członkowskich** – zgodnie z mechanizmem spójności organy nadzorcze współpracują ze sobą stosując przewidziane mechanizmy prawne: (a) kompleksowej współpracy (OneStop-Shop), (b) wzajemnej pomocy (w tym wniosków o pomoc), (c) wspólnych operacji;

20) **ustanowienie organu z uprawnieniami do dokonywania wiążącej wykładni przepisów RODO** – w miejsce Grupy Roboczej art. 29 powołano Europejską Radę Ochrony Danych, z kompetencjami w ramach mechanizmu spójności: (a) wydawania wytycznych, opinii, w tym wspólnych z EIOD, (b) rozstrzygania sporów pomiędzy organami nadzoru i wydawania wiążących decyzji, (c) doradzania KE, (d) konsultowania aktów prawnych, czy (e) organizowania konsultacji publicznych;
21) **wprowadzenie nowych gwarancji przestrzegania standardów ochrony danych** – zatwierdzonych kodeksów postępowania oraz certyfikatów wystawianych przez organ nadzorczy, bądź przez akredytowane podmioty certyfikujące.

Przegląd najważniejszych zmian systemu ochrony danych osobowych RODO – rozwinięcie

Prawo dopasowane do rodzaju administratora danych

Rozporządzenie wprowadza normy prawne mające dopasowywać system ochrony danych osobowych do jej adresatów – tzw. prawo *tailor-made* (prawo dopasowane do rodzaju jednostki organizacyjnej). RODO w szczególności dostrzega różnicę między mikro, małymi, średnimi i dużymi przedsiębiorstwami. Dotychczasowe przepisy nakazywały stosować przepisy tak samo osobom fizycznym prowadzącym jednoosobową działalność gospodarczą jak i dużym spółkom akcyjnym[191]. W efekcie większość zarówno małych podmiotów, jak i dużych korporacji nie przestrzegała w pełni przepisów z zakresu ochrony danych osobowych. W preambule do RODO w punkcie (13) podkreślono, że „aby zapewnić spójny poziom ochrony osób fizycznych w Unii oraz zapobiegać rozbieżnościom hamującym swobodny przepływ danych osobowych na rynku wewnętrznym, należy przyjąć rozporządzenie, które zagwarantuje podmiotom gospodarczym – w tym mikroprzedsiębiorstwom oraz małym i średnim przedsiębiorstwom – pewność prawa i przejrzystość. (…) Z uwagi na szczególną sytuację mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw rozporządzenie przewiduje wyjątek dotyczący rejestrowania czynności przetwarzania dla podmiotów zatrudniających mniej niż 250 pracowników. Ponadto zachęca się instytucje i organy Unii, państwa członkowskie i ich organy nadzorcze, by stosując rozporządzenie, uwzględniały szczególne potrzeby mikro oraz małych i średnich przedsiębiorstw”[192].

Rozporządzenie dostosowuje zobowiązania do rodzaju przedsiębiorstwa i uwzględnia specyfikę różnej wielkości firm – rozróżnia przede wszystkim małe oraz większe jednostki[193]. Przykładowo art. 30 rozporządzenia dotyczący konieczności rejestrowania czynności przetwarzania, który w ustępie 1 stanowi, iż każdy administrator oraz – gdy ma to zastosowanie – przedstawiciel administratora prowadzą rejestr czynności przetwarzania danych osobowych, za które odpowiadają. W myśl natomiast ustępu 2 – każdy podmiot przetwarzający oraz – gdy ma to zastosowanie – przedstawiciel podmiotu przetwarzającego prowadzą rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora. Powyższe

[191] Zob. A. Krasuski, Skolimowska D., *Dane osobowe w przedsiębiorstwie*, Warszawa 2007.

[192] Artykuł 1 – Przedmiot i cele, Motyw 13 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 (Dz. Urz. UE L 119 z dn. 4.05.2016, s. 1–88).

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

przepisy nie mają zastosowania do: (a) przedsiębiorcy lub podmiotu zatrudniającego mniej niż 250 osób, chyba że przetwarzanie, którego dokonują, może powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą, (b) nie ma charakteru sporadycznego lub (c) obejmuje szczególne kategorie danych. Innym przykładem jest możliwość wyznaczenia przez grupę przedsiębiorstw (tj. przedsiębiorstwo sprawujące kontrolę oraz przez nie kontrolowane) jednego Inspektora Ochrony Danych, o ile można będzie łatwo nawiązać z nim kontakt z każdej jednostki organizacyjnej.

Najbardziej znaczące różnice w dostosowaniu przepisów rozporządzenia do różnej wielkości przedsiębiorstw odnotować należy w dziale przewidującym kary za naruszenie przepisów. Administracyjne kary pieniężne zostały uregulowane w art. 83 rozporządzenia, stanowiącym część rozdziału VIII zatytułowanego „Środki ochrony prawnej, odpowiedzialność i sankcje". Sankcje administracyjne, w przeciwieństwie do sankcji karnych, nie mają charakteru represji za popełniony czyn – lecz swego rodzaju dolegliwości dla sprawcy naruszenia, i to niezależnie od tego, czy i jakie skutki wywołało to naruszenie. Nakładanie kar administracyjnych należy do kompetencji organu nadzorczego, przy czym może on nałożyć karę niezależnie od zastosowania innych środków naprawczych[194]. Adresatami kar mogą być następujące podmioty: (1) administrator danych[195], (2) podmiot przetwarzający dane w imieniu administratora[196], (3) podmiot certyfikujący[197] oraz (4) podmiot monitorujący[198].

Wysokość kar została określona przez wskazanie maksymalnych progów, podanych w procentach i konkretnych kwotach. Ogólne rozporządzenie o ochronie danych określa dwa maksymalne progi: wyższy i niższy (zależne od kategorii czynu). Próg niższy to 10 mln euro, a w przypadku przedsiębiorstwa – w wysokości do 2% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego. Próg wyższy to 20 mln euro i 4% obrotu (w przypadku przedsiębiorstwa). W obu przypadkach progi zostały wskazane jako maksymalne, a w przypadku obliczenia zarówno „procentowego", jak i „kwotowego", zastosowanie będzie miała kwota wyższa. RODO stanowi, że administracyjne kary pieniężne nakłada się, zależnie od okoliczności każdego indywidualnego przypadku. Jednocześnie art. 83 ust. 2 rozporządzenia wprowadza 11 kryteriów miarkowania kary. W konsekwencji procedura

[194] Do środków naprawczych należą m.in. ostrzeżenia, upomnienia, nakazy, czasowe ograniczenie przetwarzania danych, cofnięcie certyfikacji.

[195] Użyta w rozporządzeniu definicja administratora danych nie uległa istotnym zmianom w porównaniu z obecnie obowiązującą na gruncie krajowych przepisów definicji administratora danych. Administrator danych to osoba fizyczna lub prawna, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. Administrator może zostać wskazany w przepisach prawa unijnego lub krajowego, mogą też zostać w tych przepisach określone kryteria wyznaczania administratora. Szerzej nt. administratora danych zob. P. Jatkiewicz, *Ochrona danych osobowych Teoria i Praktyka*, Polskie Towarzystwo Informatyczne, Warszawa 2015.

[196] Podmiot przetwarzający to instytucja znana choćby z art. 31 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Zgodnie z RODO jest to osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora. Szerzej nt. podmiotu przetwarzającego dane w imieniu administratora zob. P. Figielski, Komentarz do art. 4 rozporządzenia nr 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 [w:] *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, red. P. Figielski, Warszawa 2018.

[197] Podmiot certyfikujący to podmiot dokonujący certyfikacji zgodności przetwarzania danych z rozporządzeniem. Akredytacją podmiotów certyfikujących zajmują się organy nadzorcze i krajowe jednostki akredytujące, działające na podstawie odrębnych przepisów. Szerzej nt. podmiotu certyfikującego zob. 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. Por. K. Szczypińska, *RODO: Wysokie wymagania wobec podmiotów certyfikujących*, https://www.prawo.pl/biznes/wymogi-erod-dla-podmiotow-certyfikujacych-katarzyna-szczypinska,366145.html, [dostęp: 17.11.2020].

[198] Podmiot monitorujący to podmiot zajmujący się monitorowaniem przestrzegania kodeksów postępowania w danym sektorze, do których tworzenia zachęca się w art. 40 rozporządzenia. Szerzej nt. podmiotu monitorującego zob. T. Grabowska, *Branżowe kodeksy postępowania i podmioty monitorujące*, https://gu.com.pl/branzowe-kodeksy-postepowania-i-podmioty-monitorujace/, [dostęp: 17.11.2020].

ustalania kar administracyjnych nie ustanawia sztywnych zasad (np. widełek), lecz opiera się na klasycznej uznaniowości organu, który korzystając ze swojej władzy dyskrecjonalnej oblicza wysokość kary wobec popełniającego delikt na prawie ochrony danych osobowych[199].

Niewątpliwie w przypadku przedsiębiorców organ musi doprowadzić do porównania wysokości kary obliczonej „kwotowo" z wysokością obliczoną „procentowo", i zestawić to z górną granicą procentowego określenia wysokości kary (w zależności od czynu – 2 lub 4% rocznego światowego obrotu). W pierwszym kroku organ ustala wysokość obrotu, następnie oblicza, ile wynosi – w zależności od rodzaju czynu – 2 lub 4% rocznego światowego obrotu. W kolejnym kroku porównuje tak ustaloną kwotę z kwotą – odpowiednio – 10 lub 20 mln euro, wreszcie wybiera wyższą z nich. Tak określona kwota stanowi podstawę do ustalenia ostatecznej wysokości kary, i to na tym etapie organ bierze pod uwagę wymienione powyżej kryteria. Ważnym jest, iż organ musi – przy ustalania wysokości kary – wziąć pod uwagę wielkość przedsiębiorcy, jego możliwości organizacyjne, przychody, poziom zatrudnienia i wszelkie inne okoliczności, które potencjalnie mogły wpłynąć na stopień zawinienia. I to właśnie w tym momencie ujawnia się relacyjność prawa do rodzaju podmiotu, w szczególności uwzględnienie różnic między mikro, małymi, średnimi i dużymi przedsiębiorstwami.

Ułatwione składanie skarg do organów nadzorczych

Rozporządzenie wprowadza ułatwienia w procedurze składania skarg do organów nadzorczych. Zgodnie z motywem 141 RODO w związku z art. 47 Karty praw podstawowych UE każda osoba, której dane dotyczą, powinna mieć prawo wniesienia skargi do jednego organu nadzorczego oraz prawo do skutecznego środka ochrony prawnej przed sądem.

Obywatel ma prawo złożyć skargę w państwie członkowskim, w którym ma miejsce zwykły pobyt, a jeżeli uzna, że jego prawa wynikające z rozporządzenia są naruszane, lub jeżeli organ nadzorczy nie reaguje na skargę, częściowo lub w całości ją odrzuca lub oddala, lub nie podejmuje działania, choć jest to niezbędne do ochrony praw tej osoby, ma prawo złożyć skargę w którymkolwiek państwie członkowskim[200]. A zatem skargę można złożyć do dowolnego organu nadzorczego na terenie Unii Europejskiej, i wtedy podmiot ten będzie brał udział w sprawie jako tzw. „zainteresowany organ nadzorczy"[201]. Jest to o tyle praktyczne, iż skargę można wnieść do organu ochrony danych osobowych np. w kraju gdzie zwykle się przebywa i pracuje lub kraju gdzie się mieszka. Ze względów proceduralnych można też wybrać kraj, w którym doszło do naruszenia praw.

---

[199] Szerzej zob. K. Szymielewicz, *Reforma europejskiego prawa o ochronie danych osobowych z perspektywy praw obywateli – więcej czy mniej ochrony?*, Monitor prawniczy 2016, nr 20.

[200] Każda osoba, której dane dotyczą, ma prawo wnieść skargę do organu nadzorczego, w szczególności w państwie członkowskim swojego zwykłego pobytu, swojego miejsca pracy lub miejsca popełnienia domniemanego naruszenia, jeżeli sądzi, że przetwarzanie danych osobowych jej dotyczące narusza rozporządzenie. Organ nadzorczy, do którego wniesiono skargę, informuje skarżącego o postępach i efektach rozpatrywania skargi, w tym o możliwości skorzystania z sądowego środka ochrony prawnej. Zob. art. 77 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 (Dz. Urz. UE L 119 z dn. 4.05.2016, s. 1–88).

[201] W przypadku transgranicznego naruszenia danych administrator powinien dokonać analizy, czy wiodącym organem nadzorczym w odniesieniu do czynności przetwarzania, które zostały objęte naruszeniem jest Prezes UODO, czy też może inny europejski organ nadzorczy. Zob. Wytyczne dotyczące ustalenia wiodącego organu nadzorczego właściwego dla administratora lub podmiotu przetwarzającego (WP 244), https://www.uodo.gov.pl/pl/10/5, [dostęp: 17.11.2020].

Postępowanie wyjaśniające na podstawie skargi powinno być prowadzone – z zastrzeżeniem kontroli sądowej – w zakresie odpowiadającym konkretnej sprawie. Organ nadzorczy powinien w rozsądnym terminie poinformować osobę, której dane dotyczą, o postępach i wynikach rozpatrywania skargi. Jeżeli dana sprawa wymaga dalszego postępowania wyjaśniającego lub koordynacji działań z innym organem nadzorczym, osoba, której dane dotyczą, powinna zostać o tym uprzednio poinformowana. Aby ułatwić wnoszenie skarg, każdy organ nadzorczy powinien zastosować takie środki jak udostępnienie formularza skargi, który można wypełnić także elektronicznie, przy czym nie należy wykluczać innych sposobów komunikacji. W myśl art. 55 rozporządzenia każdy organ nadzorczy jest właściwy do wypełniania zadań i wykonywania uprawnień powierzonych mu na terytorium swojego państwa członkowskiego.

Pod rządami RODO skargę można złożyć do organu nadzorczego bezpłatnie[202] – co niewątpliwie było wyjściem naprzeciw składanym latami postulatom. Rozporządzenie ustala, że organ nadzorczy (i każdy jego odpowiednik w innych państwach UE) ma wykonywać zadania na rzecz podmiotów danych i, jeżeli istnieje, Inspektora Ochrony Danych w sposób wolny od opłat, a opłaty mogą się pojawić tylko wtedy, gdy wnioski są ewidentnie nieuzasadnione lub nadmierne. Przy czym to na organie nadzorczym spoczywa ciężar udowodnienia, że wnioski mają taki charakter. Postępowanie przed Prezesem urzędu nadzoru w tym zakresie jest jednoinstancyjne. Jego przebieg reguluje Kodeks postępowania administracyjnego (z wyjątkami wynikającymi z ustawy o ochronie danych osobowych z 2018 roku). Choć dla przedsiębiorców ten zestaw zmian jest umiarkowanie odczuwalny, to z perspektywy osób fizycznych, których dane są przetwarzane – ułatwienia należy oceniać bardzo pozytywnie. Przykładowo pod rządami starej ustawy złożenie skargi do GIODO wymagało wniesienia opłaty skarbowej w wysokości 10 zł[203].

Ponadto obowiązkiem każdego organu nadzorczego stało się podejmowanie wszelkich czynności nakierowanych na zmaterializowanie ułatwień w zakresie wnoszenia skarg. Przykładem podejmowania takich działań jest wprowadzenie gotowego formularza skargi, który można wypełnić również elektronicznie. Tym samym skarga do Prezesa Urzędu Ochrony Danych Osobowych stała się nie tylko niemal darmowym środkiem prawnym, ale przy tym intuicyjnym i stosunkowo prostym w użyciu[204]. W Polsce zgłoszenia do PUODO można dokonać na cztery sposoby:

1) elektronicznie poprzez wypełnienie dedykowanego formularza elektronicznego dostępnego bezpośrednio na platformie biznes.gov.pl,
2) elektronicznie poprzez wysłanie formularza na skrzynkę podawczą ePUAP,

[202] Z uwagi na fakt, że większość kontroli GIODO stanowiło efekt postępowania skargowego można założyć pozytywną korelację między zniesieniem opłaty od skarg a ich ilością. Państwo członkowskie musi zapewnić by organ nadzorczy dysponował odpowiednimi zasobami ludzkimi, pozwalającymi skutecznie obsłużyć skargi. Zob. G. Sibiga, *Postępowanie w sprawach ochrony danych osobowych*, Dom Wydawniczy ABC, Warszawa 2003.
[203] Szerzej zob. M. Sakowska-Baryła, *Kontrolowanie przez GIODO przetwarzania danych osobowych*, Kontrola Państwowa 2016, nr 2.
[204] *RODO na tacy. Odcinek V: Lekcje samoobrony, czyli jak skorzystać z praw, które daje RODO*?, https://panoptykon.org/rodo-na-tacy-V, [dostęp: 15.11.2020].

3) elektronicznie poprzez wysłanie wypełnionego formularza za pomocą pisma ogólnego dostępnego na platformie biznes.gov.pl lub platformie epuap.gov.pl,
4) tradycyjną pocztą wysyłając wypełniony formularz na adres urzędu.

RYSUNEK 4 Skargi i zgłoszenia do Prezesa Urzędu Ochrony Danych Osobowych

Źródło: *Jeśli chcesz złożyć skargę…*, Urząd Ochrony Danych Osobowych, https://uodo.gov.pl/pl/83/155, [dostęp: 17.12.2020]

Wnosząc skargę nie trzeba wykazywać ani krzywdy, ani szkody z tym związanej, natomiast zaleca się sformułowanie żądań. Przykładowo można się domagać: (1) zmuszenia firmy/instytucji do tego, żeby podjęła reakcję na skierowane żądanie (np. usunęła niepotrzebne dane, udzieliła informacji, przestała przekazywać dane innym podmiotom, po wniesionym sprzeciwie); czy (2) nałożenia na nią administracyjnej kary pieniężnej.

Skarga powinna dotyczyć naruszenia przepisów ochrony danych osobowych. Prezes UODO będzie badać czy doszło do naruszenia obowiązującego prawa wyłącznie w tym zakresie. Sytuacjami, w których najczęściej narzędzie skargi, może być wykorzystywane, są wszelkie formy naruszeń oraz lekceważenia prawa osób, których dane są przetwarzane przez administratorów lub podmioty przetwarzające dane w ich imieniu (procesorzy). W szczególności można wymienić takie sytuacje jak:

- brak podania informacji na jakiej podstawie i po co przetwarzane są dane będące w dyspozycji danego podmiotu,
- brak wskazania praw jakie przysługują osobie, której dane są przetwarzane (m.in. brak poinformowania o prawie do: dostępu do swoich danych, ich sprostowania, usunięcia,

ograniczenia przetwarzania, przenoszenia, wniesienia sprzeciwu, do tego by być poinformowanym o zautomatyzowanym podejmowaniu decyzji, w tym profilowaniu, o długości przechowywania czy podania danych kontaktowych Inspektora Ochrony Danych),
- przetwarzanie danych pomimo cofnięcia zgody przez osobę, której dane dotyczą,
- brak wypełnienia obowiązku informacyjnego wobec osoby, której dane dotyczą,
- brak usunięcia danych (skorzystania z prawa do bycia zapomnianym) na zgodne z prawem i uzasadnione wezwanie w tym zakresie,
- brak poinformowania osoby, której dane dotyczą o naruszeniach, które zaszły „na tych danych" (np. wyciek danych, ich zagubienie czy udostępnienie osobom niepowołanym)
- brak zaprzestania wykorzystywania danych do celów marketingowych pomimo wniesienia sprzeciwu w tym zakresie,
- brak zaprzestania wykorzystywania danych osobowych dzieci w sytuacji braku przesłanki legalizującej przetwarzanie (np. brak zgody rodzica lub opiekuna prawnego osoby poniżej 16. roku życia na korzystanie z usług społeczeństwa informacyjnego).

Należy pamiętać, że skarga do Prezesa Urzędu powinna być poprzedzona uprzednią próbą realizacji uprawnień w kontakcie z administratorem danym lub procesorem (uzyskanie wyjaśnień lub spełnienie żądania). Dopiero prawidłowo odnotowana nieskuteczność tak podjętej próby uzasadnia skargę.

Domyślna prywatność od podstaw (privacy by design i privacy by default)

Rozporządzenie wprowadza zasady ochrony danych w fazie projektowania oraz domyślnej ochrony danych. W obecnym stanie prawnym jednak żaden akt prawny nie definiuje pojęcia „*privacy by design*" (nazywanej też „zasadą prywatności w fazie projektowania") ani „*privacy by default*" (nazywanej też „zasadą prywatności w ustawieniach domyślnych"). Ich treść oraz zakres są ustalane poprzez wskazanie funkcji, jakie spełniać powinny wprowadzane do użytku programy (systemy) przetwarzające dane osobowe.

Zasada ochrony danych w fazie tworzenia wymaga uwzględnienia gwarancji dla prywatności już na etapie projektowania jak również przez cały cykl życia usług, systemów i aplikacji – tym samym realizacji ochrony danych wpisaną w konstrukcję instrumentów (*design*). Zasada domyślnej ochrony danych wymaga natomiast systemowego podejścia do konstruowania usług, systemów i aplikacji, uwzględniającego możliwość konfiguracji ustawień prywatności przez osobę, której dane dotyczą, jednak z zastrzeżeniem, że prywatność jest w nich stanem wyjściowym (*default*).

Podstawowym celem zasady *privacy by design* jest „zaszycie" zasad ochrony prywatności w każdy projekt zakładający przetwarzanie danych osobowych w taki sposób, aby od samego początku jego istnienia ochrona prywatności stanowiła jego część składową. W praktyce wyróżnia się siedem podstawowych zasad objętych koncepcją *privacy by design*, które zostały

ostatecznie potwierdzone, na mocy Rezolucji w sprawie prywatności w fazie projektowania przyjętej przez 32 Międzynarodową Konferencję Rzeczników Ochrony Danych i Prywatności w 2010 roku[205]. Jedną z nich jest zasada *privacy by default*, która zakłada ochronę prywatności, jako domyślne ustawienie każdego programu (systemu), a zmiana takiego ustawienia powinna następować jedynie na wyraźne żądanie użytkownika programu. Tym samym *privacy by default* zawiera się w *privacy by design* i przewiduje domyślną ochronę prywatności wszystkich użytkowników danego systemu[206]. Użytkownicy chcąc zrezygnować z części swej prywatności powinni podjąć aktywne działania w tym kierunku, a nie być poddanymi ingerującym w ich prywatność decyzjom twórców systemu. Literatura przedmiotu wskazuje na siedem podstawowych zasad domyślnej prywatności.

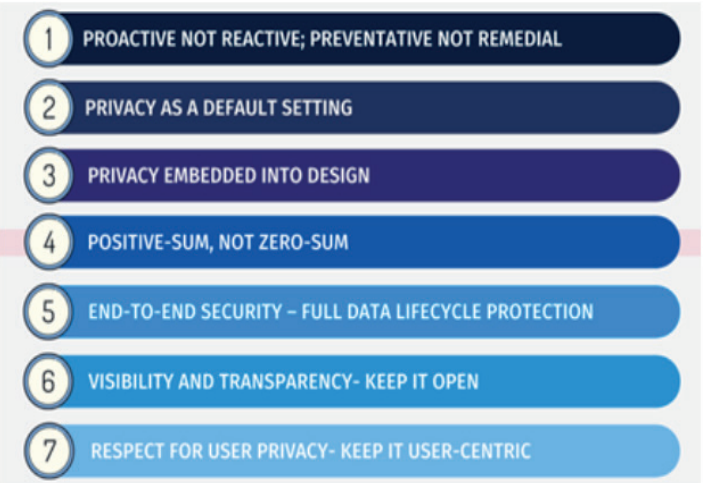
RYSUNEK 5 Privacy by design – zasady #1

1. prywatność wbudowana w projekt/przedsięwzięcie
2. podejście „użytkowniko-centryczne" (nastawione na perspektywę użytkownika)
3. unikanie fałszywych dychotomii,
4. transparentność w relacjach z użytkownikami
5. pełna ochrona w trakcie całego cyklu życia projektu/przedsięwzięcia,
6. prywatność wdrożona w ustawieniach domyślnych
7. proaktywność w zapobieganiu naruszeniom

Źródło: A. Gerunov, *Privacy by Design in Practice,* https://logsentinel.com/blog/privacy-by-design-in-practice/, [dostęp: 17.12.2020]

[205] Rezolucja ta nie zakłada egzekwowania tych zasad wobec podmiotów prywatnych. Wydaje się zatem, że do momentu rozpoczęcia stosowania rozporządzenia zasady *privacy by design* i *privacy by default* powinny być postrzegane jedynie w kategoriach dobrych i rekomendowanych praktyk. Zob. Rezolucja w sprawie prywatności w fazie projektowania przyjęta przez 32. Międzynarodową Konferencję Rzeczników Ochrony Danych i Prywatności, Jerozolima 2010.
[206] Szerzej zob. 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.

RYSUNEK 6 Privacy by design – zasady #2



1. proaktywność zamiast reaktywności – zapobieganie, nie leczenie
2. prywatność w ustawieniach domyślnych
3. prywatność osadzona/zaszyta w modelu
4. suma dodatnia nie suma zerowa
5. bezpieczeństwo od A do Z – obejmujące cały cykl życia
6. jawność, transparentność
7. poszanowanie prywatności użytkownika

Źródło: *7 principles of Privacy by Design,* https://dataprivacymanager.net/seve-principles-of-privacy-by-design-and-default-what-is-data-protection-by-design-and-default/, [dostęp: 17.12.2020]

Koncepcja *privacy by design* przeszła w ostatnich latach długą drogę – od zasady odnoszącej się początkowo jedynie do ochrony prywatności użytkowników systemów teleinformatycznych – do stanu powszechnie rozpoznawanej, jawnej[207], transparentnej i stosowanej reguły również przez organy publiczne na etapie tworzenia prawa. Zgodnie z postanowieniami rozporządzenia administrator jest zobowiązany ograniczyć zakres domyślnie przetwarzanych danych – ilości zbieranych danych, okresu ich przechowywania, ich dostępności – do danych niezbędnych dla osiągnięcia konkretnego celu przetwarzania. W szczególności zastosowane przez niego środki techniczne i organizacyjne muszą zapewnić, że dane osobowe nie będą domyślnie udostępniane bez interwencji osoby, której dotyczą. Tytułem przykładu wskazać należy, że rozszerzenie zakresu przetwarzania danych, np. widocznych dla innych użytkowników portalu społecznościowego, nie może wynikać z ustawień administratora, lecz ze zmian wprowadzonych indywidualnie przez samego użytkownika. Dotychczas praktyka zmierzała w odwrotnym kierunku. Ustawienia domyślne wprowadzane przez administratorów determinowały późniejsze ustawienia prywatności użytkowników portali społecznościowych[208].

Wprowadzenie w życie założeń zasad prywatności w fazie projektowania oraz w ustawieniach domyślnych wymaga zastosowania szeregu rozbudowanych środków technicznych

[207] Szerzej zob. C. Martysz, *Jawność i jej ograniczenia. Zasady przepływu informacji pomiędzy organami publicznymi* [w:] *Jawność i jej ograniczenia. Zadania i kompetencje*, tom 9, red. Szpor G., Szmulik B., Warszawa 2015.
[208] Szerzej zob. Wytyczne 8/2020 w sprawie targetowania użytkowników mediów społecznościowych, wersja 2.0, przyjęte 13 kwietnia 2021 r., Europejska Rada Ochrony Danych.

i organizacyjnych (takich jak np. pseudonimizacja[209]). Chodzi o minimalizację poświęcanego przez użytkowników czasu niezbędnego do określenia zakresu przetwarzanych danych – bez konieczności ingerencji przez użytkownika[210].

Dobór środków technicznych i organizacyjnych zapewniających ochronę danych w fazie projektowania i domyślną ochronę danych powinien wynikać z charakteru, zakresu, kontekstu i celów przetwarzania oraz prawdopodobieństwa wystąpienia oraz wagi naruszenia. Należy uwzględnić przy tym stan wiedzy technicznej, a więc reagować na zachodzące zmiany techniczne, przy jednoczesnym uwzględnieniu kosztów wdrażania rozwiązań i ich dostępności na rynku. Zasady *privacy by design* nie należy zawężać do obowiązku administratorów projektujących lub modyfikujących procesy przetwarzania danych w systemach teleinformatycznych[211]. Należy ją postrzegać w szerszym kontekście, obejmującym również specyfikacje w przetargach publicznych oraz przy tworzeniu prawa.

Podkreślić należy, że formą wykazania wywiązania się z obowiązku zapewnienia ochrony danych w fazie projektowania i domyślnej ochrony danych może być m.in. uzyskanie przez administratora lub procesora certyfikatu potwierdzającego zgodność operacji przetwarzania z postanowieniami rozporządzenia, w ramach zatwierdzonego mechanizmu certyfikacji określonego w art. 42 rozporządzenia.

Inspektor Ochrony Danych zamiast Administratora Bezpieczeństwa Informacji

Rozporządzenie likwiduje funkcje Administratora Bezpieczeństwa Informacji (ABI), powołując nową – Inspektora Ochrony Danych (IOD). Przy czym analiza zakresów zadań wynikających z przepisów ochrony danych osobowych wskazuje, iż błędne jest identyfikowanie funkcji ABI i IOD w sposób tożsamy. RODO wprowadza istotne zmiany kompetencyjne, które wskazują nie tylko na rozbieżność obowiązków, ale wręcz inne pole uzasadnienia funkcjonowania w ramach tych dwóch pozycji wewnątrzorganizacyjnych. O ile Administrator Bezpieczeństwa Informacji był usytuowany *pro foro interno* („do wewnątrz") jednostki organizacyjnej administratora i wykonywał obowiązki w jego imieniu i na jego rzecz[212], to już Inspektor Ochrony Danych – pomimo, iż funkcjonujący przy administratorze w ramach jego jednostki organizacyjnej – pełni rolę niezależnego wobec tegoż administratora, audytora i gwaranta prawidłowej realizacji procesów przetwarzania danych[213].

[209] Aby zachęcić do stosowania pseudonimizacji podczas przetwarzania danych osobowych, należy umożliwić stosowanie u tego samego administratora środków pseudonimizacyjnych niewykluczających ogólnej analizy, o ile administrator ten zastosował środki techniczne i organizacyjne niezbędne do tego, by rozporządzenie zostało wdrożone w zakresie danego przetwarzania i by dodatkowe informacje pozwalające przypisać dane osobowe konkretnej osobie, której dane dotyczą, były przechowywane osobno. Administrator przetwarzający dane osobowe powinien wskazać osoby uprawnione. Zob. *Anonimizacja i pseudonimizacja danych – techniki ochrony danych*, Newsletter UODO dla Inspektorów Ochrony Danych 2021, nr 4 (25), https://rodoprotektor.pl/anonimizacja-i-pseudonimizacja-danych-osobowych/, [dostęp: 17.12.2020].

[210] Kwestia domyślności już w wielu innych obszarach funkcjonuje w praktyce, przykładowo producenci domowych routerów sieci bezprzewodowej już nie ustalają takich samych haseł dla każdego urządzenia – użytkownicy często podłączali takie urządzenie i korzystali z domyślnych urządzeń. Zob. M. Bieńkowski, *7 grzechów projektowania sieci Wi-Fi*, https://www.computerworld.pl/news/7-grzechow-projektowania-sieci-Wi-Fi,413368.html, [dostęp: 19.12.2020].

[211] Szerzej zob. S. Kotecka, *Strategie i dobre praktyki dotyczące bezpieczeństwa informacji przetwarzanych w systemach teleinformatycznych i ochrony przed ich nieuprawnionym ujawnieniem* [w:] *Wybrane dobre praktyki w zakresie usług elektronicznych*, red. J. Gołaczyński, Warszawa 2016.

[212] Wyjątkiem były tzw. sprawdzenia realizowane na rzecz GIODO. Szerzej zob. K. Mystek, *Sprawdzanie dokonywane przez ABI na zlecenie GIODO*, Ekspert Ochrony Informacji 2016, nr 1 (7).

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

Zadaniem Inspektora jest monitorowanie przestrzegania przepisów o ochronie danych osobowych w jednostce, w której wykonuje funkcje. Inspektor ma informować administratora lub podmiot przetwarzający oraz wszystkich pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich. Podstawowe zadania Inspektora Ochrony Danych zostały określone w art. 39 – przy czym należy zauważyć, iż przepis nie zawiera enumeratywnego ich wyliczenia. Zadania te to m.in.:

- realizowanie obowiązków informacyjnych,
- monitorowanie przestrzegania przepisów prawa – identyfikacja i analiza procesów przetwarzania,
- informowanie, doradzanie i rekomendowanie określonych działań administratorowi lub podmiotowi przetwarzającemu,
- szacowanie ryzyka związanego z operacjami przetwarzania z uwzględnieniem charakteru, zakresu i kontekstu celów przetwarzania,
- współpraca z organem nadzorczym i pełnienie funkcji punktu kontaktowego dla organu nadzorczego,
- prowadzenie audytów wewnątrz w organizacji,
- przeprowadzanie szkoleń dla osób zatrudnionych oraz dbanie o właściwy poziom wiedzy w obszarze ochrony danych osobowych.

Jak wskazuje Maciej Kołodziej status byłego ABI oraz jego zadania w dużej części pokrywały się ze statusem i zadaniami aktualnego Inspektora określonymi w art. 37–39 RODO[214]. „Obie regulacje przewidują w tym zakresie: (1) podległość pod administratora danych, (2) wymaganie posiadania odpowiedniej wiedzy w zakresie przepisów o ochronią danych, (3) niezależność i zapewnienie niezbędnych środków do realizacji zadań, (4) nadzorowanie zgodności przetwarzania danych z przepisami, (5) zapoznawanie osób upoważnionych z przepisami o ochronią danych, (6) możliwość wykonywania dodatkowych zadań, które nie naruszają prawidłowego wykonywania zadań podstawowych, (7) informowanie urzędu o wyznaczeniu Inspektora (przekazywanie danych kontaktowych). Natomiast różnice pomiędzy funkcją Inspektora a ABI dotyczą m.in.: (1) obowiązku wyznaczenia Inspektora w określonych przypadkach (np. przez organy i podmioty publiczne), (2) ochrony Inspektora przed zwolnieniem lub ukaraniem za wykonywanie swoich zadań, (3) konsultowania oceny skutków planowanych operacji przetwarzania na ochronę danych, udzielania zaleceń oraz monitorowania jej wykonywania, (4) pełnienia funkcji punktu kontaktowego dla osób, których dane dotyczą, w sprawach dotyczących przetwarzania ich danych osobowych, (5) pełnienia funkcji punktu kontaktowego dla urzędu nadzoru, w tym w przypadkach uprzednich konsultacji w zakresie przetwarzania danych, (6) publikacji danych Inspektora, (7) podawanie informacji

[214] Zob. M. Byczkowski, *Przygotowanie ABI do nowej funkcji inspektora ochrony danych*, Informacja w administracji publicznej 2017, nr 1.

o Inspektorze w określonych przypadkach (np. w klauzulach informacyjnych)[215]. Nowością stała się możliwość powołania IOD spoza grona pracowników administratora. Dopuszczalny zatem jest również outsourcing tej funkcji. Jednocześnie IOD może zostać powołany w każdej organizacji, nawet jeśli nie jest to wymagane przepisami prawa. Na korzyść przemawia także możliwość wyznaczenia przez grupę przedsiębiorstw jednego Inspektora, pod warunkiem, że z każdej siedziby będzie można się z nim łatwo skontaktować[216].

TABELA 10 Porównanie statusu oraz zadań IOD oraz ABI – przepisy rozporządzenia ogólnego z 2016 r. i ustawy o ochronie danych osobowych z 1997 r.

Lp.	Przepis RODO	Przepis ustawy o ochronie danych osobowych z 1997 r.	Komentarz
	Wyznaczenie IOD oraz powołanie ABI		
1.	Art. 37 ust. 1 – obowiązek wyznaczenia Inspektora w trzech przypadkach. Art. 37 ust. 4 – możliwość wyznaczenia Inspektora w innych sytuacjach	Art. 36a ust. 1 – możliwość powołania ABI	Ustawa wprowadzała fakultatywność w zakresie powołania ABI. RODO wprowadza częściowy obowiązek wyznaczenia inspektora
2.	Art. 37 ust. 2 i 3 – możliwość wyznaczenia Inspektora dla grupy przedsiębiorstw oraz organów lub podmiotów publicznych	Brak regulacji w tym zakresie	Na podstawie ustawy każdy administrator może powołać tylko jednego ABI. W praktyce osoby, które pełnią taką funkcję np. w grupie kapitałowej, muszą być powołane odrębnie przez każdą ze spółek z grupy
3.	Brak regulacji w tym zakresie	Art. 36a ust. 6 – możliwość powołania zastępców ABI	Nie ma przeszkód, aby zgodnie z RODO powołać zastępców Inspektora
4.	Art. 37 ust. 5 – kwalifikacje do pełnienia funkcji Inspektora: • posiadanie wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych • umiejętność wypełnienia zadań, o których mowa w art. 39	Art. 36a ust. 5 – kwalifikacje do pełnienia funkcji ABI: • pełna zdolność do czynności prawnych oraz korzystanie z pełni praw publicznych • posiadanie odpowiedniej wiedzy w zakresie ochrony danych osobowych • niekaralność za umyślne przestępstwo	W RODO dodatkowo wymagane jest posiadanie umiejętności dotyczących wykonywania zadań Inspektora. Nie ma natomiast wymogów dotyczących niekaralności oraz zdolności do czynności prawnych i korzystania z praw publicznych
5.	Art. 37 ust. 6 – sposób zatrudnienia Inspektora: • umowa o pracę • umowa o świadczenie usług	Brak regulacji w tym zakresie	Nie ma przeszkód, aby powołany ABI na podstawie ustawy był zatrudniany w obu formach opisanych w RODO
6.	Art. 37 ust. 7 – publikacja danych kontaktowych Inspektora oraz zawiadamianie o nich urzędu nadzoru	Art. 46b – zgłoszenie powołania i odwołania ABI do rejestracji GIODO	Nie ma obowiązku w ustawie publikowania danych Inspektora. Dane publikuje GIODO w jawnym rejestrze. W RODO nie ma zapisów o prowadzeniu przez urząd nadzoru jawnego rejestru Inspektorów
	Status IOD oraz ABI		
1.	Art. 38 ust. 1 – zapewnienie włączania Inspektora we wszystkie sprawy dotyczące ochrony danych osobowych	Brak regulacji w tym zakresie	W praktyce administrator informuje ABI o działaniach związanych z przetwarzaniem danych – mogą to być zapisy wynikające z przyjętej polityki bezpieczeństwa
2.	Art. 38 ust. 2 – wsparcie Inspektora w wypełnianiu przez niego zadań, w tym zapewnienie: • zasobów niezbędnych do wykonania zadań • dostępu do danych osobowych i operacji przetwarzania • zasobów niezbędnych do utrzymania jego wiedzy fachowej Art. 38 ust. 2 zd. 1 – zapewnienie aby Inspektor nie otrzymywał instrukcji dotyczących wykonywania swoich zadań	Art. 36a ust. 8 – zapewnienie środków i organizacyjnej odrębność ABI do niezależnego wykonywania przez niego zadań	Wymogi zbieżne. RODO bardziej doprecyzowuje kwestie niezależności Inspektora oraz wsparcia w zakresie wykonywania jego zadań
3.	Art. 38 ust. 2 zd. 2 – zapewnienie, aby inspektor nie był odwoływany ani karany za wypełnianie swoich zadań	Brak regulacji w tym zakresie	
4.	Art. 38 ust. 3 zd. 3 – podległość inspektora pod administratora danych	Art. 36a ust. 7 – podległość ABI pod kierownika jednostki lub osobę fizyczną będącą administratorem danych	Wymogi zbieżne
5.	Art. 38 ust. 4 – możliwość kontaktowania się osób, których dane dotyczą, z Inspektorem	Brak regulacji w tym zakresie	W praktyce często zapytania od osób są kierowane do ABI, który nadzoruje lub wyjaśnia daną sprawę. Takie zadania można powierzyć ABI na podstawie art. 36a ust. 4 ustawy

[215] Zob. K. Syska, *Administrator bezpieczeństwa informacji a inspektor ochrony danych – porównanie przesłanek powołania, statusu i zadań*, Monitor prawniczy 2016, nr 20.

[216] *Vademecum ABI. Część II – Przygotowanie do roli Inspektora Ochrony Danych*, red. M. Kołodziej, Warszawa 2017, s. 4.

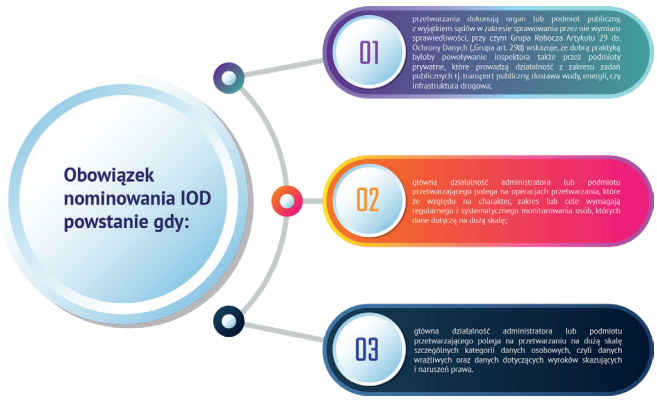
Lp.	Przepis RODO	Przepis ustawy o ochronie danych osobowych z 1997 r.	Komentarz
6.	Art. 38 ust. 5 – zobowiązanie inspektora do zachowania tajemnicy lub poufności co do wykonywania swoich zadań	Brak regulacji w tym zakresie	
	Zadania Inspektora oraz ABI		
1.	Art. 38 ust. 6 – możliwość wykonywania przez Inspektora innych zadań i obowiązków; zapewnienie, aby takie zadania i obowiązki nie powodowały konfliktu interesów	Art. 36 ust. 4 – możliwość wykonywania przez ABI innych obowiązków, jeżeli nie naruszy to prawidłowego wykonywania jego zadań	Wymogi zbieżne
2.	Art. 39 ust. 1 lit. a – informowanie osób, które przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisów o ochronie danych Unii lub państwa członkowskiego oraz doradzanie im w tej sprawie	Art. 36a ust. 2 pkt 1 lit. c – zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych	Zadania zbieżne. RODO dodatkowo wprowadza obowiązek doradzania w sprawach ochrony danych. W praktyce ABI również doradza w sprawach ochrony danych przy prowadzeniu nadzoru nad ich przetwarzaniem
3.	Art. 39 ust. 1 lit. b – monitorowanie przestrzegania RODO, innych przepisów o ochronie danych Unii lub państwa członkowskiego oraz polityk ochrony danych przyjętych przez administratora	Art. 36a ust. 2 pkt 1 lit. a i b • sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych • nadzorowanie opracowania i aktualizowania dokumentacji ochrony danych oraz przestrzegania zasad w niej określonych	Zadania zbieżne – w obu wypadkach chodzi o wykonywanie czynności weryfikujących zgodność przestrzegania przepisów o ochronie danych. RODO w przeciwieństwie do ustawy nie precyzuje trybu i sposobu wykonania tego zadania – w tym celu mogą zostać zatwierdzone kodeksy postępowania
4.	Art. 39 ust. 1 lit. c – udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania	Brak regulacji w tym zakresie	
5.	Brak regulacji w tym zakresie	Art. 36a ust. 2 pkt 2 – prowadzenie jawnego rejestru zbiorów danych osobowych	RODO wprowadza obowiązek prowadzenia przez administratora danych oraz podmiot przetwarzający rejestrów czynności przetwarzania danych osobowych – zbliżonych w swoim zakresie do rejestru zbiorów prowadzonego przez ABI. Takie zadania można powierzyć Inspektorowi zgodnie z art. 38 ust. 6 RODO
6.	Art. 39 ust. 1 lit. d – współpraca z organem nadzorczym	Brak regulacji w tym zakresie	
7.	Art. 39 ust. 1 lit. e – pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami oraz prowadzenie konsultacji we wszelkich innych sprawach	Brak regulacji w tym zakresie	
8.	Brak regulacji w tym zakresie	Art. 19b. 1 – możliwość zwrócenia się do ABI przez GIODO o dokonanie sprawdzenia zgodności przetwarzania z przepisami w określonym zakresie i terminie	
9.	Art. 39 ust. 2 – wypełnianie zadań z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania	Brak regulacji w tym zakresie	
	Podawanie informacji na temat wyznaczonego IOD oraz powołanego ABI		
1.	Art. 13 i 14 – podawanie danych kontaktowych Inspektora w klauzulach informacyjnych przy zbieraniu danych osobowych	Brak regulacji w tym zakresie	
2.	Art. 30 – podawanie danych kontaktowych Inspektora w rejestrach czynności przetwarzania danych osobowych	Brak regulacji w tym zakresie	
3.	Art. 33 – podawanie danych kontaktowych Inspektora w zawiadamianiu organu nadzorczego o naruszenia ochrony danych	Brak regulacji w tym zakresie	
4.	Art. 36 – podawanie danych kontaktowych Inspektora we wniosku do organu nadzorczego o uprzednie konsultacje	Brak regulacji w tym zakresie	
5.	Art. 47 – podawanie zadań inspektora w wiążących regułach korporacyjnych	Brak regulacji w tym zakresie	

Źródło: *Vademecum ABI. Część II – Przygotowanie do roli Inspektora Ochrony Danych*, red. M. Kołodziej, Warszawa 2017, s. 4–7

Przepis art. 37 RODO określa kryteria, które decydują o obowiązku powołania Inspektora Ochrony Danych przez administratora lub inny podmiot przetwarzający (procesora). I tak powołuje się IOD gdy:

- przetwarzania dokonują organ lub podmiot publiczny[217], z wyjątkiem sądów w ramach sprawowania przez nie wymiaru sprawiedliwości; lub
- główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania podmiotów danych na dużą skalę; lub
- główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych (takich jak dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne i światopoglądowe, przynależność do związków zawodowych, dane genetyczne, dane biometryczne, dane dotyczące zdrowia, seksualności lub orientacji seksualnej osoby), oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa.

RYSUNEK 7 Obowiązek wyznaczenia Inspektora Ochrony Danych – typologia



Źródło: *Inspektor Ochrony Danych – co się za tym kryje*, https://evosolutions.com.pl/inspektor-ochrony-danych-co-sie-za-tym-kryje/, [dostęp: 17.12.2020]

[217] Przez organy i podmioty publiczne obowiązane do wyznaczenia inspektora, o których mowa w art. 37 ust. 1 lit. a rozporządzenia 2016/679, rozumie się: (1) jednostki sektora finansów publicznych, (2) instytuty badawcze, (3) Narodowy Bank Polski. Zgodnie z art. 10 ustawy o ochronie danych osobowych podmiot, który wyznaczył inspektora, zawiadamia Prezesa Urzędu o jego wyznaczeniu w terminie 14 dni od dnia wyznaczenia, wskazując imię, nazwisko oraz adres poczty elektronicznej lub numer telefonu inspektora. Zawiadomienie może zostać dokonane przez pełnomocnika podmiotu, o którym mowa w ust. 1. Do zawiadomienia dołącza się pełnomocnictwo udzielone w formie elektronicznej. W zawiadomieniu oprócz danych, o których mowa w ust. 1, wskazuje się: (1) imię i nazwisko oraz adres zamieszkania, w przypadku gdy administratorem lub podmiotem przetwarzającym jest osoba fizyczna, (2) firmę przedsiębiorcy oraz adres miejsca prowadzenia działalności gospodarczej, w przypadku gdy administratorem lub podmiotem przetwarzającym jest osoba fizyczna prowadząca działalność gospodarczą, (3) pełną nazwę oraz adres siedziby, w przypadku gdy administratorem lub podmiotem przetwarzającym jest podmiot inny niż wskazany w pkt 1 i 2, (4) numer identyfikacyjny REGON, jeżeli został nadany administratorowi lub podmiotowi przetwarzającemu. Podmiot, który wyznaczył inspektora, zawiadamia Prezesa Urzędu o każdej zmianie danych, o których mowa w ust. 1 i 3, oraz o odwołaniu inspektora, w terminie 14 dni od dnia zaistnienia zmiany lub odwołania. W przypadku wyznaczenia jednego inspektora przez organy lub podmioty publiczne albo przez grupę przedsiębiorców, każdy z tych podmiotów dokonuje zawiadomienia, o którym mowa w ust. 1 i 4. Zawiadomienia, o których mowa w ust. 1 i 4, sporządza się w postaci elektronicznej i opatruje kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP. Podmiot, który wyznaczył inspektora, udostępnia dane inspektora, o których mowa wyżej, niezwłocznie po jego wyznaczeniu, na swojej stronie internetowej, a jeżeli nie prowadzi własnej strony internetowej, w sposób ogólnie dostępny w miejscu prowadzenia działalności. Zob. art. 37 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 (Dz. Urz. UE L 119 z dn. 4.05.2016, s. 1–88).

Z uwagi na fakt, iż rozporządzenie używa pojęć szerokich i niedookreślonych trudno wskazać punkt, czy moment, w którym materializuje się obowiązek powołania Inspektora. Z pewnością wyznaczenie Inspektora jest obligatoryjne w przypadku administratorów danych i procesorów, których główny podmiot działalności obejmuje regularne i systematyczne monitorowanie osób, których dane dotyczą przetwarzania na dużą skalę[218]. Należy zwrócić uwagę, że podmioty przetwarzające dane osobowe w imieniu administratora również są zobowiązane do wyznaczenia Inspektora Ochrony Danych. Jednocześnie wyznaczenie Inspektora jest obowiązkiem organów i podmiotów publicznych, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości[219].

Wątpliwości natomiast dotyczą tego od kiedy należy uznawać, że główna działalność polega na przetwarzaniu danych osobowych szczególnych kategorii, czy też kwestii przetwarzania danych osób zatrudnionych, które ze względu na swój charakter, zakres, cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą. Biorąc pod uwagę szeroką przestrzeń interpretacyjną przesłanek, o którym mowa powyżej, jak również szereg nowych obowiązków związanych z zapewnieniem bezpieczeństwa przetwarzania danych osobowych, wymagających profesjonalnej wiedzy i kompetencji, wydaje się, ze powołanie IOD jest – z ostrożności prawnej i organizacyjnej – powinnością. Należy przypomnieć, że powołanie ABI było w pełni dobrowolne.

Zgodnie z art 38 ust. 3 rozporządzenia wyznaczony Inspektor podlega kierownictwu administratora lub podmiotu przetwarzającego, które z kolei ma obowiązek: (1) zapewniać, by Inspektor był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych, (2) wspierać Inspektora 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 na profesjonalnym poziomie, (3) zapewniać, by Inspektor nie otrzymywał instrukcji dotyczących wykonywania tych zadań.

Zgodnie z przepisami rozporządzenia kryterium wyboru Inspektora są jego kwalifikacje zawodowe, w szczególności jego specjalistyczna wiedza z zakresu prawa i praktyk w dziedzinie ochrony danych, oraz umiejętność realizacji ustawowych zadań. „Podstawowym warunkiem powołania osoby na stanowisko IOD jest zatem wiedza fachowa na temat prawa i praktyk w dziedzinie ochrony danych. Kandydat na to stanowisko musi posiadać również umiejętności niezbędne do wykonywania obowiązujących go zadań, do czego niezbędna okazuje się wiedza na temat: innych przepisów odnoszących się do ochrony danych, systemów informatycznych, procesów przetwarzania danych oraz środków zabezpieczeń.

[218] Monitorowanie osób, których dane dotyczą, to obserwowanie ich aktywności i wyborów w Internecie oraz wykorzystywanie wynikających z tych obserwacji wniosków – profilowanie osoby fizycznej, do analiz i prognoz jej przyszłych decyzji, preferencji i zachowań. Zob. *Internet – problemy prawne*, red. R. Skubisz, Lublin 1999. Por. K. Grzybczyk, A. Auleytner, J. Kulesza, *Prawo w wirtualnych światach*, Difin, Warszawa 2013.

[219] Inspektor ochrony danych może zostać powołany na okres od 2 do 5 lat. Możliwy jest ponowny wybór tej samej osoby na stanowisko inspektora z zastrzeżeniem, że nie można sprawować funkcji dłużej niż przez 10 lat. Każda instytucja lub organ, który powoła inspektora (lub inspektorów) zobowiązana jest go zgłosić do rejestru prowadzonego przez Europejskiego Inspektora Ochrony Danych. Szerzej zob. K. Syska, *Administrator bezpieczeństwa informacji a inspektor ochrony danych – porównanie przesłanek powołania, statusu i zadań*, Monitor prawniczy 2016, nr 20.

Do skutecznego wypełniania zadań Inspektor potrzebuje ponadto podstawowej wiedzy z zarządzania (dotyczącej m.in. zarządzania czasem, podejścia procesowego), pedagogiki (transfer wiedzy), czy wiedzy na temat branży i środowiska, w jakim funkcjonuje organizacja"[220].

Inspektor może być pracownikiem na podstawie umowy o pracę lub wykonywać zadania na podstawie umowy o świadczenie usług, przy czym osoba zajmująca to stanowisko nie może realizować obowiązków, które wynikają z innych umów zawartych z administratorem. Zgodnie z art. 38 pkt 6 RODO osoba powołana na stanowisko IOD może wykonywać inne zadania i obowiązki, o ile nie powodują one konfliktu interesów z wykonywanymi zadaniami Inspektora. Stanowiska, których obejmowanie nie może łączyć się ze sprawowaniem funkcji IOD to przykładowo: dyrektor generalny, dyrektor operacyjny, dyrektor finansowy, dyrektor ds. medycznych, kierownicy działów HR, IT, czy marketingu. Inspektor Ochrony Danych Osobowych nie powinien być także członkiem zarządu ani prokurentem. Nie istnieją zatem żadne prawne obostrzenia dotyczące zlecania Inspektorowi Danych Osobowych innych zadań, natomiast należy pamiętać, że nie mogą one unicestwiać istoty jego pracy (np. prowadzenie rejestru czynności przetwarzania nie jest obowiązkiem IOD wynikającym z przepisów, natomiast wydaje się, że jest ono możliwe przy zapewnieniu właściwych zasobów do jego prowadzenia, zarówno merytorycznych, jak i czasowych). Ponad wszystko należy pamiętać, że Inspektor Ochrony Danych to funkcja niezależna. Rozporządzenie zapewnia Inspektorowi swobodę w ramach struktur wewnętrznych. Administrator i podmiot przetwarzający nie może udzielać Inspektorowi wiążących instrukcji w zakresie m.in.: rozpoznania sprawy, rodzaju podjętych środków, czy konieczności kontaktu z organem nadzorczym. Co najważniejsze w zakresie swoich obowiązków IOD podlega właścicielowi/prezesowi/zarządowi jednostki organizacyjnej.

Inspektor nie może być także odwoływany ani karany przez administratora ani podmiot przetwarzający za wypełnianie swoich zadań. Wyklucza to nakładanie na Inspektora kar służbowych za wypełnianie ustawowych funkcji. Ta gwarancja niezależności Inspektora jest niezbędna dla zapewnienia mu możliwości wykonywania zadań, obejmujących monitorowanie działań administratora lub procesora w zakresie ochronny danych osobowych, jak również innych obowiązków wskazanych w art. 39 rozporządzenia. Brak gwarancji niezależności Inspektora narażałoby go na nieformalną presję ze strony administratora danych, procesora lub zwierzchników w przypadkach, w których formułowane przez Inspektora wnioski powodowałyby konieczność ponoszenia przez te podmioty znacznych kosztów czy obciążałyby odpowiedzialnością określone osoby.

[220] W praktyce niezbędne okazują się również zdolności interpersonalne, gdyż rzeczywistą ochronę danych można zapewnić tylko przy zaangażowaniu w ten proces pracowników – świadomych zagrożeń i potrafiących na nie reagować oraz przejawiających do tego wystarczająca motywację. Zob. A. Mednis, *Ochrona prywatności i danych osobowych w przepisach prawa pracy – problemy interpretacyjne i konfrontacja z praktyką* [w:] *Ochrona danych podmiotów objętych prawem pracy i prawem ubezpieczeń społecznych*, red. Wyka T., Nerka A., Wolters Kluwer Polska, Warszawa 2012, s. 102–109.

Administrator lub podmiot przetwarzający są zobowiązani opublikować dane kontaktowe Inspektora Ochrony Danych i zawiadomić o nich organ nadzorczy. Rozporządzenie określa, że osoby, których dane się przetwarza, mogą kontaktować się z Inspektorem we wszystkich sprawach związanych z przetwarzaniem ich danych oraz z korzystaniem z praw przysługujących im na mocy rozporządzenia. Jego dane będą więc musiały znaleźć się na formularzach zgody. Rozporządzenie nie wskazuje jakie dane kontaktowe Inspektora należy podać ale wydaje się, iż podanie adresu mailowego bezpośrednio do Inspektora jest wystarczające. Artykuł 38 ust. 5 rozporządzenia wprowadza obowiązek zachowania przez Inspektora tajemnicy lub poufności w zakresie wykonywania swoich zadań.

Przyjęcie koncepcji łączenia odpowiedzialności z poziomem ryzyka (risk based approach)

Przyjęcie koncepcji podejścia opartego na ryzyku (*risk based approach*) zakłada, że podstawowym obowiązkiem zarówno administratora danych, jak i procesora jest wdrożenie odpowiednich środków technicznych oraz organizacyjnych zabezpieczających dane osobowe. Odpowiednich czyli adekwatnych do „ryzyka wiążącego się z przetwarzaniem, w szczególności wynikającego z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych”[221]. Szeroka paleta stosowanych rozwiązań technologicznych (jak np. Big Data[222], chmury obliczeniowe – *cloud computing*[223]), i w ślad za tym rosnące ryzyko związane z przetwarzaniem danych osobowych implikuje konieczność zastosowania szczególnych środków bezpieczeństwa.

Zasada podejścia opartego na ryzyku oznacza, że administratorom i podmiotom przetwarzającym nie wskazuje się ściśle określonych środków i procedur w zakresie bezpieczeństwa, np. kontroli dostępu, szyfrowania, rozliczalności czy sposobu monitorowania procesów przetwarzania. Zamiast tego zobowiązuje się ich do samodzielnego przeprowadzania szczegółowej analizy prowadzonych procesów i dokonywania samodzielnej oceny ryzyka, na jakie przetwarzanie danych w konkretnym przypadku jest narażone.

---

[221] Uwzględniając 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, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym m.in. (a) pseudonimizację i szyfrowanie danych osobowych, (b) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania, (c) zdolność do szybkiego przywrócenia dostępności danych osobowych i odstępu do nich w razie incydentu fizycznego lub technicznego, (d) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo. Zob. art. 32 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), (Dz. Urz. UE L 119 z 04.05.2016, s. 1–88).

[222] Szerzej na temat Big Data zob. M. Mattioli, *Disclosing Big Data*, Minnesota Law Review 2014, nr. 99, s. 535–583; I. Rubinstein, *Big Data: The End of Privacy or a New Beginning?*, International Data Privacy Law 2013, nr 2, s. 74–87. Por. raporty: Big data, artificial intelligence, machine learning and data protection, Information Commissioner's Office, 4.09.2017, Big Data: A Tool for Inclusion or Exclusion?, Federal Trade Commission 2016, oraz opinię: Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU, WP 221, Grupa robocza art. 29.

[223] Szerzej na temat chmur obliczeniowych zob. A. Krasuski, *Chmura obliczeniowa. Prawne aspekty zastosowania*, Warszawa 2018. Por. 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.

RYSUNEK 8 Podejście oparte na ryzyku – info i cyber sfera

Źródło: opracowanie własne na podstawie: *Risk Based Approach To Cyber And Information Security*, https://www.slideteam.net/risk-based-approach-to-cyber-and-information-security.html, [dostęp: 17.12.2021]

Im większe ryzyko związane z przetwarzaniem danych osobowych, tym większy powinien być zakres obowiązków mających na celu zabezpieczenie danych[224]. Należy zważyć, że ustawa o ochronie danych osobowych z 1997 roku nie znała takiego podejścia i wszystkich administratorów traktowała równo – nakładając na nich takie same obowiązki. Stąd większość małych administratorów oceniała zakres nałożonych obowiązków jako zbyt rygorystyczny w stosunku do skali ich działalności. Z kolei dla dużych jednostek organizacyjnych wymogi były łatwe do spełnienia. Biorąc pod uwagę zakres zabezpieczeń do wdrożenia (dodatkowo brak skutecznych sankcji za niestosowanie zasad) skutek był taki, iż większość małych administratorów w swojej działalności w zasadzie nie uwzględniała prawa ochrony danych

[224] Brak właściwego zabezpieczenia podważa zaufanie do administratora danych. Działania zabezpieczające powinny być poprzedzone analizą ryzyka zagrożenia w sferze cyberprzestrzeni i następnie wdrożeniem procedury polityki bezpieczeństwa (*security policy)*. W konstrukcję polityki bezpieczeństwa wpisuje się zatem pojęcie poziomu cyberbezpieczeństwa, tzn. określenie rodzaju, stopnia i sposobu zabezpieczenia sprzętu, oprogramowania, a tym samym danych. Wymaga to zintegrowanego podejścia do kwestii cyberbezpieczeństwa, obejmującego nie tylko sprzęt, urządzenia, procesy, procedury czy prowadzoną przez pracodawcę politykę, lecz także czynnik osobowościowy i społeczny, a więc zaangażowanych w tym procesie ludzi. Zabezpieczenie to powinno być zatem traktowane jako element zarządzania ryzykiem. Stąd jednym ze sposobów wykrywania zagrożenia w zakresie ujawniania danych osobowych jest stałe monitorowanie sfery zarówno zewnętrznej, jak i wewnętrznej. Szerzej zob. M. Rojszczak, *Ochrona prywatności w cyberprzestrzeni z uwzględnieniem zagrożeń wynikających z nowych technik przetwarzania informacji*, Wolters Kluwer, Warszawa 2019. Por. B. Iwaszko, *Bezpieczeństwo systemów teleinformatycznych*, IT w Administracji 2012, nr 12; B. Iwaszko, *Bezpieczeństwo szczególnie wymagane*, IT w Administracji 2012, nr 9. Zob. też 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 oraz Oświadczenie 2/2021 w sprawie nowych postanowień Konwencji Rady Europy o cyberprzestępczości (Konwencja Budapeszteńska), przyjęte 2 lutego 2021 r., Europejska Rada Ochrony Danych.

osobowych. Z drugiej strony potężne podmioty przetwarzające ogromne zasoby danych, przy wdrożeniu minimalnych wymogów, miały poczucie spełnienia obowiązków ustawowych.

Rozporządzenie starało się wyjść naprzeciw oczekiwaniom związanym z dyferencjacją obowiązków w zależności od wielkości administratora i zakresu przetwarzanych danych. „Nowe przepisy odchodzą od jednakowego traktowania wszystkich podmiotów w zakresie obowiązku zabezpieczania danych osobowych. Nakazują one dostosowanie zabezpieczeń do ryzyk związanych z przetwarzaniem danych osobowych, które u każdego z administratorów mogą być inne. Zastępują one w tym zakresie obecne podejście legalistyczne, które szczegółowo określa zabezpieczenia, jakie powinni wdrożyć administratorzy danych osobowych, by być zgodni z prawem. W praktyce podejście oparte na ryzyku oznacza, że administratorzy będą musieli samodzielnie oceniać pod względem ryzyka procesy przetwarzania danych, posiadane systemy informatyczne, a także swoich kontrahentów oraz dobierać odpowiednie zabezpieczenia w stosunku do zagrożeń z nimi związanych. Podejście to może być najbardziej efektywnym narzędziem ochrony danych, a także zapewniać najwyższy stopień ochrony w stosunku, zarówno do zagrożeń, jak i możliwości administratorów danych. Umożliwia ono wszystkim administratorom danych samodzielne zdecydowanie o zaangażowaniu środków w obszarach, w których ryzyko naruszenia zabezpieczeń czy praw osób, których dane dotyczą jest dla nich największe. Dzięki niemu organizacje mogą priorytetyzować zadania oraz odpowiednio kierować zasoby w celu minimalizacji największych ryzyk. W stosunku do podejścia legalistycznego, podejście oparte na ryzyku wymaga bardziej całościowego spojrzenia na ochronę danych osobowych, a nie ograniczania się tylko do wdrożenia zabezpieczeń określonych przez prawo. Brak precyzyjnych wytycznych ze strony ustawodawcy unijnego jest spowodowany częstą zmianą zagrożeń oraz sposobów ochrony przed nimi. Środki zabezpieczeń powinny gwarantować 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 (integralność i poufność)”[225].

Zasada podejścia opartego na ryzyku zobowiązuje do:

- respektowania praw i wolności osób, których dane są przetwarzane,
- dostosowania środków ochrony przetwarzania danych osobowych do skali ryzyka,
- koncentrowania się na poszukiwaniu środków redukujących prawdopodobieństwo wystąpienia zagrożeń oraz środków redukujących skutki ich wystąpienia.

Stare przepisy nakazywały dostosowanie zabezpieczeń do ryzyka związanego z przetwarzaniem danych osobowych, które u każdego z administratorów mogą przecież być i najczęściej są inne. Wdrożenie podejścia opartego na ryzyku jest w swojej istocie uruchomieniem procesu

[225] M. Chodorowski, *Największe wyzwanie RODO – on risk based approach*, https://s4edu.pl/pl/centrum-wiedzy/92-gdpr/116-najwieksze-wyzwanie-rodo-on-riks-based-approach, [dostęp: 30.05.2020]. Por. M. Malicka, *Podejście oparte na ryzyku czyli Risk Based Approach*, http://przetwarzaniedanych.pl/podejscie-oparte-na-ryzyku-czyli-risk-based-approach/, [dostęp: 30.05.2020].

wymagającego stałej identyfikacji i szacowania poziomu ryzyka związanego z przetwarzaniem danych. Zasada ta wymusza na administratorze danych i podmiocie przetwarzającym dbanie o odpowiednią ochronę na wszystkich etapach przetwarzania danych osobowych, tj. podczas całego cyklu życia informacji, od momentu zbierania danych aż do ich usunięcia. Innymi słowy konieczne jest wbudowanie zasad ochrony danych osobowych w każdy projekt zakładający przetwarzanie, a następnie zapewnienie odpowiedniego bezpieczeństwa na każdym etapie procesu przetwarzania. Takie podejście umożliwia skoncentrowanie się na sytuacjach najwyższego ryzyka, przy jednoczesnym zachowaniu odpowiedniego poziomu ochrony, gdy to ryzyko jest niskie i nie wymaga uruchomienia całego instrumentarium środków sankcyjnych przewidzianych rozporządzeniem. Pozwala to administratorom samodzielne zadecydować o zaangażowaniu środków w obszarach, w których ryzyko naruszenia praw osób, których dane dotyczą jest największe[226]. Dzięki temu organizacje mogą samodzielnie się zadaniować oraz odpowiednio kierować zasoby w celu minimalizacji ryzyk[227].

Należy podkreślić, iż w celu wywiązywania się z obowiązków płynących z przyjęcia tej zasady można stosować zatwierdzone kodeksy postępowania (art. 40 rozporządzenia[228]), lub zatwierdzone mechanizmy certyfikacji (art. 42 rozporządzenia[229]).

[226] Poradnik RODO. Podejście oparte na ryzyku. *Jak rozumieć podejście oparte na ryzyku cz. 1.*, file:///C:/Users/adwok/Downloads/Jak%20rozumie%C4%87%20podej%C5%9Bcie%20oparte%20na%20ryzyku%20wed%C5%82ug%20RODO_.pdf, [dostęp: 17.11.2020].

[227] Poradnik RODO. Podejście oparte na ryzyku. *Jak rozumieć podejście oparte na ryzyku cz. 2.*, https://rodo-hr-consulting.com.pl/wp-content/uploads/2019/03/C*z%C4%99%C5%9B%C4%87–2.-Poradnik-RODO-Podej%C5%9Bcie-oparte-na-ryzyku.pdf, [dostęp: 17.11.2020].

[228] Państwa członkowskie, organy nadzorcze, Europejska Rada Ochrony Danych oraz Komisja zachęcają do sporządzania kodeksów postępowania mających pomóc we właściwym stosowaniu rozporządzenia – z uwzględnieniem specyfiki różnych sektorów dokonujących przetwarzania oraz szczególnych potrzeb mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw. Zrzeszenia i inne podmioty reprezentujące określone kategorie administratorów lub podmioty przetwarzające mogą opracowywać lub zmieniać kodeksy postępowania lub rozszerzać ich zakres, aby doprecyzować zastosowanie rozporządzenia, między innymi w odniesieniu do: (a) rzetelnego i przejrzystego przetwarzania; (b) prawnie uzasadnionych interesów realizowanych przez administratorów w określonych kontekstach; (c) zbierania danych osobowych; (d) pseudonimizacji danych osobowych; (e) informowania opinii publicznej i osób, których dane dotyczą; (f) wykonywania przez osoby, których dane dotyczą, przysługujących im praw; (g) informowania i ochrony dzieci oraz sposobu pozyskiwania zgody osoby sprawującej władzę rodzicielską lub opiekę nad dzieckiem; (h) środków i procedur, oraz środków zapewniających bezpieczeństwo przetwarzania; i) zgłaszania organowi nadzorczemu naruszeń ochrony danych osobowych oraz zawiadamiania o takich naruszeniach osób, których dane dotyczą; j) przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych; lub k) postępowań pozasądowych oraz innych trybów rozstrzygania sporów w celu rozstrzygania sporów między administratorami a osobami, których dane dotyczą, w zakresie przetwarzania, bez uszczerbku dla praw osób, których dane dotyczą. Poza administratorami lub podmiotami przetwarzającymi, którzy podlegają rozporządzeniu, zatwierdzonych kodeksów postępowania, mogą przestrzegać także administratorzy lub podmioty przetwarzające, którzy nie podlegają rozporządzeniu, w celu zapewnienia odpowiednich zabezpieczeń w ramach przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych. Zob. art. 40 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 (Dz. Urz. UE L 119 z dn. 4.05.2016, s. 1–88). Por. Wytyczne 1/2019 dotyczące kodeksów postępowania i podmiotów monitorujących zgodnie z RODO, wersja 2.0, przyjęte 4 czerwca 2019 r., Europejska Rada Ochrony Danych.

[229] 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 rozporządzeniem operacji przetwarzania prowadzonych przez administratorów i podmioty przetwarzające. Przy tym uwzględnia się szczególne potrzeby mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw. Mechanizmy certyfikacji oraz znaki jakości i oznaczenia w dziedzinie ochrony danych zatwierdzone na mocy ust. 5 artykułu, które mają zastosowanie do administratorów lub podmiotów przetwarzających podlegających rozporządzeniu, mogą być ustanowione do wykazania odpowiednich zabezpieczeń przez administratorów lub podmioty przetwarzające, którzy zgodnie z art. 3 nie podlegają rozporządzeniu, w ramach przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych na warunkach określonych w art. 46, ust. 2, lit. f) rozporządzenia. Tacy administratorzy lub takie podmioty przetwarzające podejmują wiążące i egzekwowalne zobowiązania – w drodze umowy lub poprzez inne prawnie wiążące instrumenty – do stosowania tych odpowiednich zabezpieczeń, w tym w odniesieniu do praw osób, których dane dotyczą. Certyfikacja jest dobrowolna, a proces jej uzyskania musi być przejrzysty. Certyfikacja przewidziana w niniejszym artykule nie wpływa na spoczywający na administratorze lub podmiocie przetwarzającym obowiązek przestrzegania rozporządzenia i pozostaje bez uszczerbku dla zadań i uprawnień organów nadzorczych właściwych na mocy art. 55 lub 56 rozporządzenia. Certyfikacji dokonują podmioty certyfikujące, o których mowa w art. 43 rozporządzenia, lub dokonuje jej właściwy organ nadzorczy – na podstawie kryteriów zatwierdzonych przez niego zgodnie z art. 58, ust. 3 rozporządzenia lub przez Europejską Radę Ochrony Danych zgodnie z art. 63 rozporządzenia. W przypadku gdy kryteria są zatwierdzane przez Europejską Radę Ochrony Danych, może to skutkować wspólną certyfikacją, europejskim znakiem jakości ochrony danych. Administrator lub podmiot przetwarzający, którzy poddają swoje przetwarzanie mechanizmowi certyfikacji, udzielają podmiotowi certyfikującemu, lub gdy ma to zastosowanie – właściwemu organowi nadzorczemu wszelkich informacji i wszelkiego dostępu do swoich czynności przetwarzania, które to informacje i dostęp są niezbędne do przeprowadzenia procedury certyfikacji. Certyfikacji administratora lub podmiotu przetwarzającego udziela się na maksymalny okres 3 lat; certyfikację można przedłużyć na tych samych warunkach, o ile nadal spełnione są stosowne wymogi. W stosownym przypadku organy certyfikujące, lub właściwy organ nadzorczy cofają certyfikację, jeżeli jej wymogi nie są spełnione lub przestały być spełniane. Europejska Rada Ochrony Danych gromadzi w rejestrze wszystkie mechanizmy certyfikacji oraz znaki jakości i oznaczenia w dziedzinie ochrony danych i udostępnia je opinii publicznej za pomocą odpowiednich środków. Zob. art. 42 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 (Dz. Urz. UE L 119 z dn. 4.05.2016, s. 1–88). Por. Oświadczenie 4/2021 w sprawie umów międzynarodowych obejmujących przekazywanie danych, przyjęte 13 kwietnia 2021 r., Europejska Rada Ochrony Danych.

Proponowane do wdrożenia środki ochrony ocenia się pod kątem utraty poufności, integralności i dostępności danych, biorąc przy tym pod uwagę ich zakres, szczególne znaczenie (wrażliwość) oraz kontekst i cele przetwarzania, a tym samym także kwestie zapewniania bezpieczeństwa usług przetwarzania (niezawodność, integralność i dostępność systemu przetwarzania) oraz zapewniania autentyczności i rozliczalności danych i podmiotów uczestniczących w przetwarzaniu.

Zapewnienie poufności, integralności, dostępności, rozliczalności, autentyczności, niezaprzeczalności, niezawodności danych, dekodować można poprzez język norm, w tym w szczególności PN-ISO/IEC-17799:2005 oraz PN-I-13335–1; natomiast tworzenie i wdrażanie Systemu Bezpieczeństwa Danych Osobowych oprzeć można się na podejściu procesowym określonym w normie PN-ISO/IEC 27001, jako czterofazowy model „planuj/wykonuj/sprawdzaj/działaj". Należy przy tym mieć na uwadze, że wszelkie obowiązki wynikające z wdrożenia zasady *risk based approach* zostały wpisane również w ogólne obowiązki administratora danych, o których mowa w art. 24 rozporządzenia. „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 rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane. Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki, obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych"[230].

I tak administrator winien podejmować wszelkie niezbędne działania mające zapobiec zagrożeniom, w szczególności takim, jak: (1) sytuacje losowe, w tym nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu, jak np. pożar, zalanie pomieszczeń, katastrofa budowlana, kradzież, włamanie, (2) niewłaściwe parametry środowiska, zakłócające pracę urządzeń elektronicznych (nadmierna wilgotność, wysoka lub niska temperatura, oddziaływanie pola elektromagnetycznego, itp.), (3) awarie sprzętu lub oprogramowania, niewłaściwe działanie procedur serwisowych w tym przyzwolenie na naprawę sprzętu zawierającego dane osobowe poza siedzibą administratora, (4) naruszenie bezpieczeństwa danych przez ich nieautoryzowane przetwarzanie, (5) ujawnienie osobom nieupoważnionym zasad ochrony danych, (6) celowe lub przypadkowe rozproszenie danych w sieci publicznej (Internecie) z ominięciem zabezpieczeń systemu lub z wykorzystaniem błędów systemu, (7) zewnętrzne ataki przeprowadzane poprzez sieć publiczną (Internet), (8) naruszenia i nieprzestrzegania zasad określonych w dokumentacji ochrony danych osobowych przez osoby upoważnione do przetwarzania danych[231]. Administrator w szczególności jest zobowiązany do wdrożenia

[230] Zob. art. 24 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), Dz. Urz. UE L 119 z 04.05.2016, s. 1–88.

[231] W tym m.in.: (a) naruszenie bezpieczeństwa danych przez nieautoryzowane ich przetwarzanie, (b) ujawnienie osobom nieupoważnionym zasad ochrony danych stosowanych przez Administratora Danych, względnie bezpośrednio danych przetwarzanych, w tym również nieumyślne ujawnienie danych osobom przebywającym bez nadzoru lub w pomieszczeniach niedostatecznie nadzorowanych, (c) niewykonywanie kopii zapasowych, (d) przetwarzanie danych osobowych niezgodnie z celem, w tym w szczególności w celach prywatnych, (e) wprowadzanie zmian do systemu informatycznego, w tym np. instalowanie programów

(a) środków ochrony fizycznej danych[232], oraz (b) środków sprzętowych infrastruktury informatycznej i telekomunikacyjnej ochrony danych[233].

Zgodnie z art. 25 rozporządzenia „uwzględniając 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, administrator – zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania – wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi rozporządzenia 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. W szczególności środki te zapewniają, by domyślnie dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych”[234].

Przy tym należy mieć świadomość, że dobór środków technicznych i organizacyjnych winien uwzględniać najbardziej aktualny stan wiedzy, a zatem wychodzić naprzeciw oczekiwaniom związanych z dynamiką zmian technologicznych. RODO identyfikuje różne poziomy ryzyka. W motywie 76 preambuły do rozporządzenia wymienia się kategorie ryzyka i wysokiego ryzyka. W praktyce obowiązuje również kategoria „niskiego ryzyka”. Identyfikuje się ją na podstawie sformułowań art. 27 ust. 2 lit. a oraz art. 33 ust. 1 rozporządzenia. Dotyczą one wyłączenia obowiązku ustanowienia przedstawiciela w UE przez administratorów lub podmioty przetwarzające niemających jednostek organizacyjnych na terenie UE oraz obowiązku powiadomienia organu nadzorczego o naruszeniu ochrony danych. Trzeba tu jednak zauważyć, że przepisy zezwalające na niestosowanie się do wymienionych obowiązków mówią o małym prawdopodobieństwie wystąpienia ryzyka naruszenia praw i wolności, czyli o sytuacji, gdy

bez zgody Administratora Danych, czy Administratora Systemu Informatycznego, (f) niezabezpieczanie danych osobowych lub systemu informatycznego służącego do ich przetwarzania przed opuszczeniem miejsca pracy lub zakończeniem pracy. Zob. *Metody zabezpieczeń danych osobowych oraz miejsca ich przetwarzania w Uniwersytecie Jagiellońskim*, https://iod.uj.edu.pl/newsletter/-/journal_content/56_INSTANCE_xQD2n5noK0Fo/138774264/139386871, [dostęp: 10.12.2020]. Por. *RODO zabezpieczenia techniczne systemów informatycznych*, https://www.spark-it.pl/blog/rodo-zabezpieczenia-techniczne-systemow-informatycznych/, [dostęp: 10.12.2020].

[232] Przykładowo: (a) zbiory danych osobowych przechowywane są w pomieszczeniach zabezpieczonych drzwiami zwykłymi (niewzmacnianymi, nie przeciwpożarowymi); (b) pomieszczenia, w których przetwarzane są zbiory danych osobowych wyposażone są w system alarmowy przeciwwłamaniowy; (c) zbiory danych osobowych w formie papierowej przechowywane są w zamkniętej niemetalowej szafie; (d) kopie zapasowe/archiwalne zbiorów danych osobowych przechowywane są w zamkniętej niemetalowej; (e) pomieszczenia, w którym przetwarzane są zbiory danych osobowych zabezpieczone są przed skutkami pożaru za pomocą wolnostojącej gaśnicy; (f) dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów. Zob. *ABC zabezpieczania danych osobowych – środki techniczne i organizacyjne*, https://cognitio.edu.pl/abc-zabezpieczania-danych-osobowych-srodki-techniczne-i-organizacyjne/, [dostęp: 10.12.2020].

[233] Przykładowo: (a) dostęp do systemów operacyjnych komputerów, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła; (b) zobowiązano pracowników do okresowej ręcznej zmiany haseł; (c) zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity; (d) użyto system Firewall do ochrony dostępu do sieci komputerowej; (e) zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe. Zob. A. Nowak, *Wymogi informatyczne RODO*, http://bezowijania.com/wymogi-informatyczne-rodo, [dostęp: 10.12.2020]. Szerzej por. *Internet. Prawno-informatyczne problemy sieci, portali i e*-usług, red. G. Szpor, W. Wiewiórowski, CH Beck, Warszawa 2012.

[234] Zob. art. 25 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), Dz. Urz. UE L 119 z 04.05.2016, s. 1–88.

oceniający może dojść do wniosku, że ryzyko nie wystąpi w ogóle (*is unlikely to result in a risk to the rights and freedoms of natural persons)*. Z tego punktu widzenia należy raczej mówić o sytuacjach: brak ryzyka – ryzyko – wysokie ryzyko, przy czym administrator bądź podmiot przetwarzający ocenia prawdopodobieństwo wystąpienia ryzyka lub wysokiego ryzyka. Stwierdzenie wysokiego poziomu ryzyka naruszenia praw i wolności osób, których dane są przetwarzane, wymaga przeprowadzenia oceny skutków dla ochrony danych, podczas której należy dodatkowo uwzględnić: (a) czy operacja przetwarzania jest niezbędna, oraz (b) czy ingerencja w prywatność związana z przetwarzaniem danych jest proporcjonalna do celów przetwarzania[235].

Jeżeli z przetwarzaniem wiąże się wysokim ryzykiem naruszenia praw i wolności osób fizycznych, przeprowadzenie oceny skutków tego przetwarzania jest obowiązkowa. Jednocześnie, w rozporządzeniu wskazano trzy rodzaje przetwarzania, które podlegają ocenie. Prawodawca uznał więc z góry, że ryzyko wynikające z tych operacji jest wysokie[236].

Należy zauważyć, że zasada *risk based approach* obdarza administratorów i procesorów sporą dozą zaufania przenosząc na nich ciężar dokonania autooceny w zakresie ryzyk i powierzając decyzyjność w zakresie niezbędnych środków do wdrożenia. W tym względzie spotyka się również z krytyką, w aspekcie zdolności administratorów do prawidłowej projekcji możliwości organizacyjnych i finansowych. „Podejście oparte na ryzyku, mimo jego wielu zalet posiada też jedną poważną wadę – jest mocno subiektywne. Samodzielne dostosowywanie przez administratorów danych zabezpieczeń do ryzyka, bez posiadania przez nich odpowiednich wytycznych może być w dużej mierze dokonywane niewłaściwe. Ma to znaczenie w szczególności w przypadku małych i średnich przedsiębiorców, których świadomość w zakresie ochrony danych osobowych jest wciąż na dość niskim poziomie. Podmioty te mogą mieć duże problemy przy identyfikacji ryzyka związanego z ochroną danych, a także z dobraniem odpowiednich zabezpieczeń w stosunku do nich. W tym też zakresie mogą zdarzać się sytuacje, w których przedsiębiorcy mimo dołożenia należytej staranności w zakresie zabezpieczeń i tak staną się ofiarami incydentów godzących w ochronę danych. Powyższy problem został zauważony również podczas prac nad projektem nowych polskich przepisów. Projekt polskiej ustawy wdrażającej rozporządzenie przyznaje organowi nadzorczemu uprawnienia do opracowywania niewiążących wykazów dobrych praktyk dotyczących odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie odbywało się zgodnie z rozporządzeniem oraz polską ustawą"[237].

[235] Szerzej na temat proporcjonalności zob. M. Korycka, *Zasada proporcjonalności – refleksje na gruncie aksjologicznych podstaw Konstytucji z 1997 roku i orzecznictwa Trybunału Konstytucyjnego* [w:] *Wykładnia prawa i inne problemy filozofii prawa*, red. Morawski L., Toruń 2005, s. 43–58. Por. Opinia 01/2014 w sprawie stosowania pojęć konieczności i proporcjonalności oraz ochrony danych w sektorze egzekwowania prawa, WP 211, przyjęta 27 lutego 2014 r., Grupa robocza art. 29

[236] A. Mednis, *Wymóg oceny skutków przetwarzania w ogólnym rozporządzeniu o ochronie danych*, Monitor Prawniczy 2016, nr 20, s. 27.

[237] *Projekt ustawy o ochronie danych osobowych z marca 2017*, https://mc.gov.pl/files/projekt_ustawy_o_ochronie_danych_osobowych_28.03.2017.pdf, [dostęp: 30.05.2020]. Szerzej zob. *Ochrona danych osobowych – poradnik dla małych i średnich przedsiębiorców*, red. P. Sikorski, Polska Agencja Rozwoju Przedsiębiorczości, Warszawa 2017.

Likwidacja obowiązku kategoryzowania zbiorów danych i ich rejestrowania

Pod reżimem prawnym ustawy o ochronie danych osobowych z 1997 roku jednym z ustawowych zadań Generalnego Inspektora Ochrony Danych Osobowych było prowadzenie jawnego „Ogólnokrajowego rejestru zbiorów danych osobowych" (art. 12 ust. 3). Realizując to zadanie GIODO przyjmował m.in. zgłoszenia zbiorów do rejestracji, a w przypadku spełnienia wymogów formalnych, wpisywał zbiór do prowadzonego rejestru[238]. Tylko będący zbiorem danych osobowych usystematyzowany zestaw danych podlegał zgłoszeniu, przy czym obowiązek ten ciążył na administratorze danych. Aby zatem rozważać konieczność zarejestrowania zestawu danych należało uprzednio dokonać jednoznacznej jego klasyfikacji jako zbioru w rozumieniu przepisów ustawy o ochronie danych osobowych. Zbiorem danych osobowych, zgodnie z art. 7 pkt 1 ustawy, był każdy posiadający strukturę zestaw danych o charakterze osobowym dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten był rozproszony lub podzielony funkcjonalnie. Cechą wyróżniającą zbiór danych od innego zestawu była zatem struktura, czyli uporządkowanie według konkretnych kryteriów. Zwolnienia od generalnej zasady rejestracji zbiorów danych osobowych określone zostały w art. 43 ust. 1 pkt 1–11 ustawy[239].

Należy wyeksponować, iż koncepcja budowania zbiorów danych była fundamentem systemu ochrony danych osobowych do 2018 roku. Zaczynając pracę nad wdrożeniem odpowiednich procedur bezpieczeństwa danych osobowych, koniecznym było w pierwszej kolejności wyodrębnienie, z pośród wszystkich danych przetwarzanych przez administratora, konkretnych zbiorów[240]. Bez wyodrębnienia niemożliwe było efektywne wdrożenie procesów mających zapewnić odpowiedni poziom ochrony danych., a w konsekwencji nie można było mówić o jakiejkolwiek ochronie danych, albowiem nie było możliwe stworzenie dokumentacji bezpieczeństwa, a w ślad za tym wdrożenie jej postanowień, czy wreszcie przeprowadzenie – przewidzianych prawem – sprawdzeń i audytów. Przykładowo system upoważnień do przetwarzania

[238] Zgodnie z art. 44 ust. 1 ustawy o ochronie danych osobowych z 1997 roku zbiór mógł zostać wpisany do rejestru jeżeli postępowanie rejestracyjne wykazało, że nie zachodziła żadna z przesłanek odmawiających rejestracji. Zgłoszenia zbioru do rejestracji należało dokonać przed rozpoczęciem przetwarzania danych, czyli przed pierwszą czynnością, jaką administrator może wykonać na danych, tj. przed pozyskaniem pierwszych danych do zbioru. Jednak gdy administrator danych zamierzał przetwarzać tzw. dane szczególne to, zgodnie z art. 46 ust. 2 ustawy, mógł rozpocząć przetwarzanie dopiero po zarejestrowaniu zbioru. Zgłoszenia zbioru danych dokonywano na formularzu, którego wzór stanowił załącznik do rozporządzenia Ministra Spraw Wewnętrznych i Administracji. Zgłoszenie powinno zawierać wszystkie informacje, o których mowa w art. 41 ust. 1 pkt 1–7 ustawy i być podpisane przez administratora danych (lub inną osobę upoważnioną do reprezentowania wnioskodawcy. Zob. art. 41 rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz.U. z 2008r. Nr 229, poz. 1536).

[239] Z obowiązku rejestracji zbioru danych zwolnieni byli administratorzy następujących kategorii danych: (1) zawierających informacje niejawne, które zostały uzyskane w wyniku czynności operacyjno-rozpoznawczych przez funkcjonariuszy organów uprawnionych do tych czynności, (2) przetwarzanych przez właściwe organy dla potrzeb postępowania sądowego oraz na podstawie przepisów o Krajowym Rejestrze Karnym, przetwarzanych przez Generalnego Inspektora Informacji Finansowej, przetwarzanych przez właściwe organy na potrzeby udziału Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym, (3) dotyczących osób należących do kościoła lub innego związku wyznaniowego, o uregulowanej sytuacji prawnej, przetwarzanych na potrzeby tego kościoła lub związku wyznaniowego, (4) przetwarzanych w związku z zatrudnieniem u nich, świadczeniem im usług na podstawie umów cywilnoprawnych, a także dotyczących osób u nich zrzeszonych lub uczących się, (5) dotyczących osób korzystających z ich usług medycznych, obsługi notarialnej, adwokackiej, radcy prawnego, rzecznika patentowego, doradcy podatkowego lub biegłego rewidenta, (6) tworzonych na podstawie przepisów dotyczących wyborów do Sejmu, Senatu, Parlamentu Europejskiego, rad gmin, rad powiatów i sejmików województw, wyborów na urząd Prezydenta RP, wójta, burmistrza, prezydenta miasta oraz dotyczących referendum ogólnokrajowego i referendum lokalnego, (7) dotyczących osób pozbawionych wolności na podstawie ustawy, w zakresie niezbędnym do wykonania tymczasowego aresztowania lub kary pozbawienia wolności, (8) przetwarzanych wyłącznie w celu wystawienia faktury, rachunku lub prowadzenia sprawozdawczości finansowej, (9) powszechnie dostępnych, (10) przetwarzanych w celu przygotowania rozprawy wymaganej do uzyskania dyplomu ukończenia szkoły wyższej lub stopnia naukowego, (11) przetwarzanych w zakresie drobnych bieżących spraw życia codziennego. Zob. art. 43 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 1997r. Nr 133, poz. 883 z późn. zm.).

[240] W treści nieobowiązującego już rozporządzenia Ministra Spraw Wewnętrznych i Administracji wprost wskazano, że niezbędnym elementem Polityki Bezpieczeństwa jest wykaz zbiorów danych osobowych. Zob. § 4 pkt 2 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. z 2004r. Nr 100, poz. 1024).

danych osobowych opierał się na zapewnieniu dostępu do konkretnych zbiorów. Nie inaczej legalizowanie przetwarzania danych w oparciu o jedną z przesłanek (art. 23 lub 27 ustawy) zestawiano z zakresem przedmiotowym poszczególnych zbiorów. Wyodrębnianie zbiorów danych odbywało się w oparciu o dobrane kryteria oraz ogólne zasady (proporcjonalności, konieczności dostępu itp.[241]). Stąd zestawianie danych realizowano poprzez dostosowanie dostępu do zbiorów wyłączenie dla osób, dla których było to niezbędne w relacji do zakresu i potrzeb przetwarzania, oraz podstawy prawnej.

RYSUNEK 9 Przykładowe zestawienie wyodrębnionych zbiorów danych (zatrudnienie)

Źródło: B. Tchórzewska, *Zbiór danych osobowych dzisiaj i według RODO*, https://blog-daneosobowe.pl/zbior-danych-osobowych-charakterystyka-pojecia/, [dostęp: 17.11.2020]

RODO choć rezygnuje z konieczności budowania bezpieczeństwa danych u administratora w oparciu o konieczność zestawienia zbiorów danych, to oczywiście nie likwiduje obowiązku administratora w zakresie wdrożenia odpowiednich środków technicznych i organizacyjnych mających na celu ochronę danych osób fizycznych. Art. 24 rozporządzenia jasno precyzuje, 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 rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane. Tym samym nie nakazuje ale też nie zakazuje budowania

[241] Na temat wykładni zasady proporcjonalności zob. wyrok TK z 09.06.1998, sygn. K 28/97, OTK 1998, nr 4, poz. 50. Por. wyrok TK z 20.11.2002, sygn. K 41/02, OTK-A 2002, nr 6, poz. 83 (nieproporcjonalna ingerencja w sferę prywatności zmienionych przepisów podatkowych).

systemu w oparciu o wyodrębnienie zbiorów danych osobowych. W praktyce jednak dochodzi do zastąpienia zbiorów danych na rzecz nowego systemu zapewniania bezpieczeństwa danych w oparciu o obowiązek prowadzenia w przypadku:

- administratora danych – rejestru czynności przetwarzania danych (art. 30 ust. 1),
- procesora – rejestru kategorii czynności przetwarzania danych (art. 30 ust. 2).

Oba dokumenty nie mają jednak charakteru publicznego, podlegającego obowiązkowi notyfikacji, czy rejestracji w organie administracji publicznej. Rejestr czynności przetwarzania należy udostępnić organowi nadzorczemu jedynie na jego wyraźne żądanie (np. w czasie kontroli). Środek ciężkości zatem został przesunięty z poziomu organu oraz momentu początku przetwarzania ustawionego *ex ante* na samego administratora i ewentualną kontrolę *ex post*.

W tym kontekście powstało pytanie o to, jak należy rozróżniać „czynność przetwarzania danych" od „zbioru danych". Problemem jest to, że zarówno w treści rozporządzenia, jak i nowej polskiej ustawy nie wprowadzono wyraźnej definicji. Posiłkować się można tutaj różnymi opracowaniami, w których pojawia się odniesienie do celów przetwarzania (podobnie jak przy zbiorach). Jak wskazuje np. rekomendacja wydana przez belgijski urząd ochrony danych „czynności przetwarzania to konkretne działania podejmowane na danych w ramach każdego z celów. Jeżeli celem byłoby przesyłanie informacji handlowej drogą elektroniczną, to czynnością przetwarzania byłoby pozyskiwanie, odczytywanie, utrwalanie, przesyłanie oraz modyfikowanie danych w tym celu. W tym zakresie można by uznać, że w ramach każdego z celów przetwarzania danych mamy do czynienia z co najmniej dwoma czynnościami, jak pozyskanie oraz odczytanie danych osobowych"[242]. To pierwsza z możliwych interpretacji. „Druga z możliwych dróg interpretacji przemawia za postawieniem znaku równości pomiędzy terminem czynności przetwarzania a cel przetwarzania. W tym zakresie wykładnia pojęcia czynność zbliżałaby się do wykładni pojęcia zbioru, gdyż w praktyce obecnie zbiory wyodrębnianie są w oparciu o kryterium celu przetwarzania danych osobowych. W motywie 23 preambuły do RODO wskazuje się, że czynność przetwarzania wiąże się z oferowaniem takim osobom towarów lub usług, z kolei w motywie 24, że czynność przetwarzania można uznać za monitorowanie zachowania osób. Powyższe przemawiałoby za opowiedzeniem się za drugim z możliwych sposobów wykładni"[243].

Choć kwestia normatywna pozostaje otwarta to na podstawie dotychczasowego dorobku doktryny i orzecznictwa można przyjąć, iż niegdyś jeden zbiór oznaczał jeden cel, przy czym aktualnie im bliżej wyodrębnionemu zbiorowi do jednego celu, tym bliżej do wyodrębnionej czynności przetwarzania, której obowiązek rejestrowania już wynika z RODO. Wraz z rozpoczęciem stosowania ogólnego rozporządzenia o ochronie danych zniesiono zatem, obowiązek

[242] Rekomendacja Nr 06/2017 z 14 czerwca 2017 r. wydana przez belgijski urząd ochrony danych osobowych (Komisja ds. Prywatności), https://www.gegevensbeschermingsautoriteit.be/publications/recommandation-n-06–2017.pdf, [dostęp: 18.10.2020].

[243] *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, red. P. Litwiński, Warszawa 2018.

zgłaszania do rejestracji zbiorów danych osobowych. Oznacza to, że od tego dnia nie trzeba już przesyłać do Generalnego Inspektora Ochrony Danych Osobowych:

- zgłoszeń zbiorów danych osobowych do rejestracji,
- zgłoszeń zmian w zbiorach,
- wniosków o wykreślenie.

Wygaszenie niewygodnego i obciążającego obowiązku nie wymagało podejmowania żadnych działań po stronie przedsiębiorców. W szczególności nie trzeba było składać żadnych pism ani wniosków o wykreślenie zbiorów[244]. Z perspektywy administratorów zmianę należy oceniać pozytywnie. Procedura rejestracji i aktualizacji zbiorów często była uciążliwa i jednocześnie nie gwarantowała, prawidłowości przetwarzania i zabezpieczenia danych[245].

Konieczność dokonywania oceny skutków przetwarzania (privacy impact assessment)

Ocena skutków przetwarzania danych jest mechanizmem, który ma na celu szacowanie prawdopodobieństwa naruszenia praw i wolności osób w związku z przetwarzaniem ich danych osobowych. Mechanizm ten został uregulowany w art. 35 i 36 RODO. Arwid Mednis, dokonując wykładni ocenia, że „obydwa artykuły składają się na sekcję 3 pt. *Ocena skutków dla ochrony danych i uprzednie konsultacje*, stanowiącą część rozdziału IV poświęconego administratorowi i podmiotowi przetwarzającemu. Sam fakt wydzielenia tej tematyki oraz umieszczenie jej po sekcji 2 poświęconej bezpieczeństwu danych, a przed sekcją poświęconą Inspektorowi Ochrony Danych świadczy o wadze, jaką prawodawca unijny przywiązuje do samodzielnej oceny ryzyka związanego z przetwarzaniem danych osobowych"[246].

Ocena skutków dla ochrony danych, na podstawie art. 35 ust. 1 RODO, powinna być przeprowadzona, jeżeli dany rodzaj przetwarzania może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Wysokie prawdopodobieństwo ryzyka może wynikać z charakteru przetwarzania, a także jego zakresu, kontekstu i celu. W szczególności dotyczy to przetwarzania danych osobowych z użyciem nowych technologii, czyli tzw. przetwarzania zautomatyzowanego. Może obejmować m.in. przetwarzanie danych w celach marketingowych, w celach dostosowywania oferty do preferencji zakupowych klientów, przetwarzania danych szczególnych kategorii, a także monitorowania pracowników[247].

Jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności

[244] M. Dela, Rejestracja zbioru danych osobowych, Kwartalnik Naukowy Prawo Mediów Elektronicznych 2010, nr 2, s. 47–52. http://www.bibliotekacyfrowa.pl/Content/38667/PDF/010.pdf, [dostęp: 19.10.2020].

[245] *Znika obowiązek rejestracji zbiorów w GIODO w zamian obowiązek rejestrowania czynności przetwarzania*, https://odo24.pl/blog-post.znika-obowiazek-rejestracji-zbiorow-w-giodo-w-zamian-obowiazek-rejestrowania-czynnosci-przetwarzania2, [dostęp: 19.10.2020].

[246] A. Mednis, *Wymóg oceny skutków przetwarzania...*, s. 28.

[247] Szerzej zob. 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.

osób fizycznych, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę. Administrator może przeprowadzać oceny skutków przetwarzania w oderwaniu od całego systemu ochrony danych osobowych oraz dla tzw. dobrych praktyk. Powinien on, zgodnie z RODO, jednak:

1) konsultować dokonywanie oceny z Inspektorem Ochrony Danych, jeżeli takiego powołał (art. 35 ust. 2),
2) uwzględniać przestrzeganie zatwierdzonych kodeksów postępowania, o których mowa w art. 40 RODO (art. 35 ust. 8),
3) w stosownych przypadkach zasięgnąć również opinii osób, których dane dotyczą, lub ich przedstawicieli w sprawie zamierzonego przetwarzania, bez uszczerbku dla ochrony interesów handlowych lub publicznych lub bezpieczeństwa operacji przetwarzania (art. 35 ust. 9),
4) dokonywać przeglądu oceny w razie zmiany ryzyka wynikającego z danej operacji przetwarzania, stwierdzić, czy przetwarzanie odbywa się zgodnie z dotychczasową oceną skutków dla ochrony danych (art. 35 ust. 11).

Obowiązek przeprowadzenia oceny zależy zatem w pierwszej kolejności od wstępnej oceny ryzyka naruszenia praw i wolności osób fizycznych. Jeśli ryzyko naruszenia jest wysokie, to ocena ta staje się obowiązkową. W trzech przypadkach rozporządzenie przesądza o konieczności dokonania oceny, niezależnie od tego, jak administrator ocenia ryzyko w konkretnym przypadku. Oceny skutków należy zawsze dokonywać, gdy:

- stosuje się profilowanie[248],
- przetwarza się dane wrażliwe na dużą skalę[249],
- monitoruje się na dużą skalę miejsca publiczne[250].

[248] „Profilowanie" oznacza dowolną formę 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. Zob. art. 4 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 (Dz. Urz. UE L 119 z dn. 4.05.2016, s. 1–88).

[249] Rozporządzenie nie definiuje pojęcia „dużej skali", jednak pewne wskazówki można znaleźć w motywie 91 preambuły rozporządzenia 2016/679, w którym jako operację przetwarzania o dużej skali wskazuje się operacje służące przetwarzaniu znacznej ilości danych osobowych na szczeblu regionalnym, krajowym lub ponadnarodowym i które mogą wpłynąć na dużą liczbę osób. W tym samym motywie wskazuje się, 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. W takich przypadkach ocena skutków dla ochrony danych nie powinna być obowiązkowa. I tu również należy podkreślić, że nawet w przypadku przetwarzania danych na niewielką skalę przez niedużego administratora, jeśli dojdzie on do wniosku, że przetwarzanie danych wiąże się z wysokim ryzykiem naruszenia praw i wolności, powinien dokonać oceny skutków. Zob. motyw 91 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 (Dz. Urz. UE L 119 z dn. 4.05.2016, s. 1–88).

[250] Motyw 91 preambuły rozporządzenia wskazuje, że chodzi o monitoring realizowany w szczególności za pomocą urządzeń optyczno-elektronicznych. Przy czym należy uznać, że monitoring miejsc publicznych na dużą skalę za pomocą innych środków technicznych również będzie wymagać dokonania oceny skutków. Zob. motyw 91 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 (Dz. Urz. UE L 119 z dn. 4.05.2016, s. 1–88). Por. Wytyczne 3/2019 w sprawie przetwarzania danych osobowych za pomocą urządzeń wideo, wersja 2.0, przyjęte 29 stycznia 2020 r., Europejska Rada Ochrony Danych.

W doktrynie wskazuje się, że ocena skutków danej operacji przetwarzania jest obowiązkowa również w przypadku gdy: (1) dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych[251], (2) planowane przetwarzanie objęte jest wykazem rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych. Wykaz jest ustalany i publikowany przez organ nadzorczy.

Komentatorzy zwracają także uwagę na fakt, że ocena skutków dotyczy „nie tyle przetwarzania danych w ogóle, ile konkretnych operacji przetwarzania, związanych np. z wprowadzaniem na rynek nowej usługi, nowej aplikacji, wdrożeniem nowego systemu informatycznego itp. Rozporządzenie nie precyzuje, w jaki sposób ma być przeprowadzana ocena skutków, ani w jakiej formie mają zostać przedstawione jej rezultaty. Zważywszy na względy dowodowe oraz prawdopodobieństwo konsultacji wyników oceny z organem nadzorczym należy przyjąć, że ocena powinna powstać jako dokument na trwałym nośniku. Odpowiedzialnym za dokonanie oceny jest administrator. Rozporządzenie wyraźnie wskazuje, że Inspektor Ochrony Danych nie będzie odpowiedzialny za przeprowadzenie oceny. Jego rola sprowadzi się do konsultacji, udzielania zaleceń na żądanie wykonującego ocenę, do monitorowania jej wykonania oraz do pełnienia roli punktu kontaktowego dla organu nadzorczego w ramach konsultacji będących następstwem oceny[252]. Inspektor nie przeprowadza więc oceny skutków, administrator wykonuje ją innymi siłami, ewentualnie powierza jej wykonanie podmiotowi zewnętrznemu. Art. 35 ust. 7 rozporządzenia określa minimalną zawartość oceny skutków"[253]. I tak powinna ona zawierać co najmniej:

1) systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie – prawnie uzasadnionych interesów administratora,
2) ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów,
3) ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą,
4) środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa, mające zapewnić ochronę danych osobowych i wykazać przestrzeganie rozporządzenia, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy.

[251] RODO ustanawia zasadę ogólną: ocena skutków jest konieczna, jeśli administrator uzna, że istnieje duże prawdopodobieństwo, iż planowana operacja (rodzaj) przetwarzania pociągnie za sobą wysokie ryzyko naruszenia praw i wolności. Zakłada się zatem, że administrator dokonuje wstępnej oceny planowanej operacji, w ramach której bierze pod uwagę charakter przetwarzania (m.in. środki przetwarzania), zakres przetwarzania (m.in. rodzaj danych osobowych, ilość danych), kontekst (m.in. podstawę prawną, wpływ na podmioty danych, tj. korzyści lub ich brak) oraz cele przetwarzania (np. to, czy administrator spełnia cele prywatne czy publiczne). Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę. Gdyby jednak pomiędzy takimi operacjami upłynęło dużo czasu lub znacznie zmieniły się okoliczności przetwarzania danych, wówczas należy ponownie rozważyć przeprowadzenie oceny skutków. Zob. art. 35 ust. 1 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 (Dz. Urz. UE L 119 z dn. 4.05.2016, s. 1–88). Szerzej zob. 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

[252] Zob. art. 39 ust. 1 lit. 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 (Dz. Urz. UE L 119 z dn. 4.05.2016, s. 1–88).

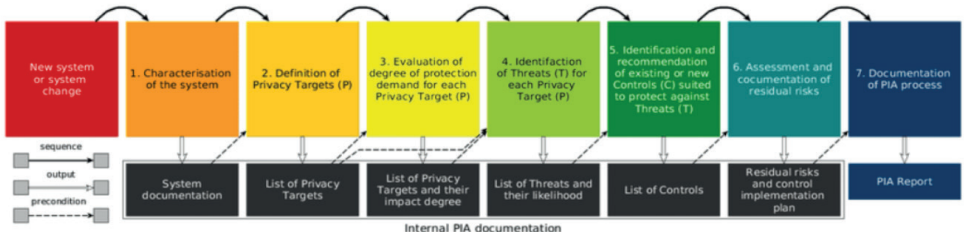
[253] A. Mednis, *Wymóg oceny skutków przetwarzania…*, s. 29–32.

TABELA 11 Proces i dokumentacja Oceny skutków przetwarzania danych – metodologia

Proces Oceny skutków przetwarzania danych							
Nowy system lub zmiana systemu	Charakterystyka systemu	Zdefiniowanie celów prywatności (*Privacy Targets*)	Ewaluacja poziomów zabezpieczeń wymaganych dla każdego z celów prywatności	Identyfikacja zagrożeń (*Treats*) dla każdego z celów prywatności	Identyfika-cja oraz rekomen-dacja narzędzi bezpiecze-ństwa wobec zagrożeń	Audyt i ocena ryzyk rezydualnych	Dokumenta-cja procesu Oceny skutków dla ochrony danych (*PIA*)
Sekwencja Rezultat Warunki brzegowe	**Dokumentacja Oceny skutków ochrony danych**						
	Doku-menta-cja systemu	Lista celów prywatności (*Privacy Targets*)	Lista celów prywatności i ich poziomu wpływu (*Impact degree*)	Lista zagrożeń oraz ich prawdopodobieństwa wystąpienia	Lista kontrolna	Ryzyko rezydualne oraz plan imple-mentacji narzędzi bezpie-czeństwa	Raport Oceny skutków ochrony danych (*PIA Report*)

Źródło: opracowanie własne na podstawie: L. Horn Iwaya, *Privacy Impact Assessment (PIA) methodology overview*, https://www.researchgate.net/figure/Privacy-Impact-Assessment-PIA-methodology-overview_fig1_330031552, [dostęp: 17.12.2020]

RYSUNEK 10 Privacy Impact Assessment (PIA) – metodologia



Źródło: L. Horn Iwaya, *Privacy Impact Assessment (PIA) methodology overview*, https://www.researchgate.net/figure/Privacy-Impact-Assessment-PIA-methodology-overview_fig1_330031552, [dostęp: 17.12.2020]

Co do zasady wymóg oceny skutków przetwarzania nie ma zastosowania do przetwarzania na mocy niezbędności wykonania obowiązku prawnego ciążącego na administratorze oraz wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi. Ocena może być jednak wymagana, jeżeli państwo członkowskie uzna za niezbędne, by przed podjęciem czynności przetwarzania dokonać oceny skutków dla ochrony danych (art. 35 ust. 10 RODO). Przepis wskazuje, że organ nadzorczy ma obowiązek doprecyzowania, jakie operacje przetwarzania podlegają ocenie skutków przetwarzania. Organ może także ustanowić i podać do wiadomości publicznej wykaz rodzajów operacji przetwarzania niepodlegających wymogowi dokonania oceny skutków dla ochrony danych. Ustalenie tego wykazu nie jest obowiązkowe. Wykaz ustala się w formie decyzji, której projekt organ przedstawia Europejskiej Radzie Ochrony – powołanej na mocy rozporządzenia. Organ może zasięgnąć opinii Rady w sprawie tego wykazu, jeżeli wykaz wywołuje skutki w więcej niż jednym państwie członkowskim. Zasięgnięcie opinii w sprawie czynności nieobjętych obowiązkiem oceny nie jest obowiązkowe i może nastąpić w dowolnym momencie, również po ustaleniu i opublikowaniu wykazu. Jeżeli wykazy rodzajów operacji przetwarzania niepodlegających wymogowi dokonania oceny skutków dla ochrony danych obejmują czynności przetwarzania związane z oferowaniem

towarów lub usług osobom, których dane dotyczą, lub z monitorowaniem ich zachowania w kilku państwach członkowskich lub mogące znacząco wpłynąć na swobodny przepływ danych osobowych w Unii, przed przyjęciem takich wykazów właściwy organ nadzorczy stosuje mechanizm spójności, o którym mowa w art. 63 RODO. Obydwa wykazy organ nadzorczy przekazuje wspomnianej Europejskiej Radzie Ochrony Danych[254].

Zgodnie z art. 35 ust. 4 rozporządzenia organ nadzorczy (w przypadku Rzeczypospolitej Polskiej Prezes Urzędu Ochrony Danych Osobowych), ma za zadanie ustanowić i podać do publicznej wiadomości wykaz operacji przetwarzania podlegający wymogowi dokonania oceny skutków dla ochrony danych. Powinien także przekazać wykaz ten Europejskiej Radzie Ochrony Danych Osobowych. Delegacja ustawowa do wydania komunikatu przez PUODO znalazła się w krajowej ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych (w art. 54 ust. 1 pkt. 1). Na podstawie art. 172 ustawy Prezes Urzędu Ochrony Danych Osobowych miał trzy miesiące od wejścia w życie ustawy na wydanie pierwszego komunikatu. Pierwszy wykaz został ogłoszony 24 sierpnia 2018 r. w Monitorze Polskim jako Komunikat Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 sierpnia 2018 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony[255]. Powyższy wykaz został zmieniony nowym, opublikowanym w dniu 8 lipca 2019 r., kiedy to w Monitorze Polskim został ogłoszony Komunikat Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 czerwca 2019 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony[256]. Dodatkowo, fakultatywnie, na podstawie art. 54 ust. 1 pkt. 2 ustawy o ochronie danych osobowych, PUODO może ustanowić i podać do publicznej wiadomości wykaz rodzajów przetwarzania niepodlegających wymogowi dokonania oceny skutków dla ochrony danych. Analogicznie do wykazu operacji podlegających ocenie, wykaz ten należy przekazać Europejskiej Radzie Ochrony Danych Osobowych (przewiduje to art. 35 ust. 5 RODO).

Pierwotny wykaz rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony zestawiał dziewięć kategorii operacji:

1) ewaluacja lub ocena, w tym profilowanie i przewidywanie (analiza behawioralna) w celach wywołujących negatywne skutki prawne, fizyczne, finansowe lub inne niedogodności dla osób fizycznych,

[254] Jeżeli wykazy operacji przetwarzania, zarówno podlegających, jak i niepodlegających ocenie skutków, obejmują czynności dokonywane w kontekście ponadgranicznym, tj. 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 tzw. mechanizm spójności, który określa sposób uzgadniania i podejmowania rozstrzygnięć przez poszczególne organy nadzorcze w różnych krajach, z udziałem Europejskiej Rady Ochrony Danych (art. 63 i nast. rozporządzenia). Zob. art. 35 ust. 6 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 (Dz. Urz. UE L 119 z dn. 4.05.2016, s. 1–88).

[255] Komunikat Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 sierpnia 2018 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony, Monitor Polski dnia 24 sierpnia 2018 r., poz. 827, https://monitorpolski.gov.pl/M2018000082701.pdf, [dostęp: 07.12.2020].

[256] Komunikat Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 czerwca 2019 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony, Monitor Polski dnia 8 lipca 2019 r., poz. 666, https://monitorpolski.gov.pl/M2019000066601.pdf.pdf, [dostęp: 07.12.2020].

2) zautomatyzowane podejmowanie decyzji wywołujących skutki prawne, finansowe lub podobne istotne skutki,
3) systematyczne monitorowanie na dużą skalę miejsc dostępnych publicznie wykorzystujące elementy rozpoznawania cech lub właściwości obiektów, które znajdą się w monitorowanej przestrzeni (do tej grupy systemów nie są zaliczane systemy monitoringu wizyjnego, w których obraz jest nagrywany i wykorzystywany tylko w przypadku potrzeby analizy incydentów naruszenia prawa),
4) przetwarzanie szczególnych kategorii danych osobowych i dotyczących wyroków skazujących i czynów zabronionych,
5) dane przetwarzane na dużą skalę, gdzie pojęcie dużej skali dotyczy:
   - liczby osób, których dane są przetwarzane,
   - zakresu przetwarzania,
   - okresu przechowywania danych,
   - geograficznego zakresu przetwarzania,
6) przeprowadzanie porównań, ocena lub wnioskowanie na podstawie analizy danych pozyskanych z różnych źródeł,
7) przetwarzanie danych dotyczących osób, których ocena i świadczone im usługi są uzależnione od podmiotów lub osób, które dysponują uprawnieniami władczymi i/lub oceniającymi,
8) innowacyjne wykorzystanie lub zastosowanie rozwiązań technologicznych lub organizacyjnych,
9) gdy przetwarzanie samo w sobie uniemożliwia osobom, których dane dotyczą, wykonywanie prawa lub korzystanie z usługi lub umowy[257].

Aktualny wykaz z dnia 17 czerwca 2019 roku uzupełnia katalog o trzy dodatkowe operacje przetwarzania danych osobowych wymagające oceny skutków przetwarzania dla ich ochrony (łącznie zatem jest tych operacji 12):

1) przetwarzanie danych biometrycznych wyłącznie w celu identyfikacji osoby fizycznej bądź w celu kontroli dostępu,
2) przetwarzanie danych genetycznych,
3) przetwarzanie danych lokalizacyjnych.

Niewątpliwie dokonanie oceny skutków wymaga zaangażowania wiedzy specjalistycznej, w tym profesjonalnego zespołu specjalistów w tym zakresie. Przedsiębiorcy, bez zewnętrznej wiedzy eksperckiej, trudno samemu dokonać rzetelnej oceny, na którą ma składać się m.in.: (1) systematyczny opis planowanych operacji przetwarzania i ich

[257] Zob. R. Stępniewski, *Ocena skutków przetwarzania – komunikat PUODO*, https://www.politykabezpieczenstwa.pl/pl/a/ocena-skutkow-przetwarzania-komunikat-puodo, [dostęp: 18.11.2020]. Por. *Artykuł 35 – Ocena skutków dla ochrony danych*, GDPR.PL, https://gdpr.pl/baza-wiedzy/akty-prawne/interaktywny-tekst-gdpr/artykul-35-ocena-skutkow-dla-ochrony-danych, [dostęp: 13.12.2020].

celów, w tym, gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez administratora[258]; (2) ocena proporcjonalności operacji przetwarzania w stosunku do celów[259], (3) ocena ryzyka naruszenia podstawowych praw i wolności osób, których dane dotyczą[260], (4) ocena środków mających zmniejszyć zagrożenia i mających chronić dane osobowe w tym zabezpieczenia, oraz (5) środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie rozporządzenia 2016/679, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą.

Z obowiązku należy zauważyć, że rozporządzenie przewiduje wyjątki od obowiązku dokonywania oceny skutków przetwarzania[261].

Przy tym należy wyeksponować, że ocena skutków nie jest zbieżna z przeprowadzanymi na podstawie aktualnych przepisów audytami ochrony danych, które zwykle stanowią kontrolę zgodności przetwarzania danych z prawem. Ocena skutków polega w znacznym stopniu na przewidywaniu wszystkich niekorzystnych skutków danej operacji dla interesów podmiotów danych. Stąd w stosownych przypadkach administrator zasięga opinii osób, których dane dotyczą, lub ich przedstawicieli w sprawie zamierzonego przetwarzania, bez uszczerbku dla ochrony interesów handlowych, publicznych lub bezpieczeństwa operacji przetwarzania. Należy także pamiętać, że już w trakcie przetwarzania, które było poddane

[258] „Prawnie uzasadniony interes" (ang. *legitimate interest)* stanowi odwołanie do przesłanki legalności, o której mowa w art. 6, ust. 1, lit. f rozporządzenia. Jeśli administrator działa na podstawie innej przesłanki legalności, wówczas nie musi jej opisywać, jednak wydaje się, że przytoczenie podstawy prawnej w ocenie skutków jest w większości przypadków konieczne, choćby w sytuacji, gdy cel przetwarzania wynika z przepisu prawa. Opisanie prawnie uzasadnionego interesu to np. wskazanie, że dopasowanie reklam do potrzeb konkretnych klientów wymaga profilowania tych osób. Szerzej zob. *Przetwarzanie danych na podstawie prawnie uzasadnionego interesu*, https://lexdigital.pl/przetwarzanie-danych-na-podstawie-uzasadnionego-interesu, [dostęp: 13.12.2020].

[259] Administrator musi uzasadnić m.in. dlaczego do danego celu niezbędne jest wykorzystanie danych identyfikujących konkretne osoby. W przypadku wykonywania obowiązku wynikającego z przepisu prawa, niezbędne jest wskazanie, dlaczego zadanie to wymaga przetwarzania danych osobowych oraz wykazanie, że danego celu nie da się osiągnąć w inny sposób. Wymóg proporcjonalności oznacza, że w ocenie należy wskazać, iż zakres danych użytych w danej operacji przetwarzania jest adekwatny do celu. Zob. W. Krawiec, *Co za dużo to nie RODO – ile danych osobowych naprawdę wolno przetwarzać?*, https://lassotakrawiec.pl/wiedza/co-za-duzo-to-nie-rodo-ile-danych-osobowych-naprawde-wolno-przetwarzac/, [dostęp: 13.12.2020].

[260] Można uznać, że to najważniejszy punkt oceny skutków, ponieważ od niego zależy dalsze postępowanie i losy ocenianej operacji. Jeśli potwierdzi się wysoki poziom ryzyka naruszenia, wówczas konieczne będą konsultacje z organem nadzorczym. Tu należy wziąć pod uwagę zagrożenia, jakie może nieść dana operacja i ocenić ryzyko ich wystąpienia („zwykłe" lub „wysokie"). Podpowiedź co do możliwych zagrożeń wynikających z przetwarzania znajdziemy w motywie 75 preambuły rozporządzenia 2016/679. Chodzi o naruszenia mogące 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; lub jeżeli przetwarzane są dane osobowe osób wymagających szczególnej opieki, w szczególności dzieci; jeżeli przetwarzanie dotyczy dużej ilości danych osobowych i wpływa na dużą liczbę osób, których dane dotyczą. Szerzej zob. Wytyczne Grupy Roboczej art. 29 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 art. 29, 17/PL WP 248 rev.01. Por. R. Stępniewski, *Jak ocenić ryzyko naruszenia praw lub wolności osób fizycznych na wypadek stwierdzenia naruszenia?*, https://www.politykabezpieczenstwa.pl/pl/a/jak-ocenic-ryzyko-naruszenia-praw-lub-wolnosci-osob-fizycznych-na-wypadek-stwierdzenia-naruszenia, [dostęp: 13.12.2020].

[261] W pewnych przypadkach niezależnie od wyników wstępnej oceny ryzyka, a także w sytuacjach, w których rozporządzenie przewiduje obowiązek oceny, można ten obowiązek wyłączyć. Dla takiego wyłączenia muszą być jednak spełnione następujące warunki: (1) przetwarzanie odbywa się na mocy art. 6, ust. 1 lit. c) (tj. przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze) lub lit. e) (tj. przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi); (2) przetwarzanie ma podstawę prawną w prawie Unii lub w prawie państwa członkowskiego, któremu podlega administrator, i prawo takie reguluje daną operację przetwarzania lub zestaw operacji i 3) oceny skutków dla ochrony danych dokonano już w ramach oceny skutków regulacji w związku z przyjęciem tej podstawy prawnej – chyba, że państwa członkowskie uznają za niezbędne, aby przed podjęciem czynności przetwarzania dokonać oceny skutków dla ochrony danych. Innymi słowy, ocena mogłaby być dokonywana na etapie legislacyjnym lub po przyjęciu aktu prawnego, ale przed rozpoczęciem przetwarzania. Tu może pojawić się wątpliwość co stanie się w sytuacji, gdy np. ustawa będzie regulować nowy rodzaj przetwarzania danych, a ocena skutków będzie wykonana już po przyjęciu ustawy i ocena wykaże wysokie ryzyko naruszenia praw i wolności. Konsultacje z organem mogą doprowadzić do wniosku, że przetwarzanie naruszy przepisy rozporządzenia. W takiej sytuacji organ będzie mógł zakazać przetwarzania pomimo ustawowej podstawy takiej operacji. Zob. art. 35 ust. 10 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 (Dz. Urz. UE L 119 z dn. 4.05.2016, s. 1–88).

ocenie, może zmienić się ryzyko naruszeń praw i wolności. W takiej sytuacji administrator powinien dokonać przeglądu przetwarzania, aby stwierdzić, czy przetwarzanie odbywa się zgodnie z oceną skutków dla ochrony danych.

Ponadto w stosownym przypadku administrator zasięga opinii podmiotów danych lub ich przedstawicieli w sprawie zamierzonego przetwarzania, zaś jeśli ocena skutków wskaże, że przetwarzanie niosłoby duże zagrożenie, gdyby administrator nie przedsięwziął środków w celu zminimalizowania tego zagrożenia, to przed przetworzeniem danych osobowych administrator konsultuje się z organem nadzorczym. Oznacza to, że z ostrożności proceduralnej administrator winien w razie wątpliwości skonsultować się z organem nadzorczym w przedmiotowej kwestii.

Konsultację należy przeprowadzić przed rozpoczęciem przetwarzania danych, tzn. przed ich zgromadzeniem lub, jeśli dane są już wykorzystywane przez administratora dla innego celu, przed przystąpieniem do ich wykorzystania do celu objętego oceną skutków. Konsultacje z organem prowadzi administrator, nawet jeśli w przetwarzaniu bierze udział podmiot przetwarzający dane w imieniu administratora. Administrator powinien w ramach konsultacji przekazać organowi nadzorczemu następujące informacje: (1) opis obowiązków administratora oraz – jeśli ma to zastosowanie – obowiązków współadministratorów i podmiotów przetwarzających uczestniczących w przetwarzaniu, w szczególności w przypadku przetwarzania w ramach grupy przedsiębiorstw, (2) cele i sposoby zamierzonego przetwarzania, (3) środki i zabezpieczenia mające chronić prawa i wolności osób, których dane dotyczą, (4) jeśli administrator powoła Inspektora Ochrony Danych – dane kontaktowe tegoż Inspektora, (5) ocenę skutków dla ochrony danych oraz (6) wszelkie inne informacje, których żąda organ nadzorczy.

Administrator – co do zasady – jest ograniczony czasowo terminem planowanego rozpoczęcia danej operacji przetwarzania. Jeśli zrezygnuje z przetwarzania danych, wówczas nie jest zobowiązany do konsultacji z organem. Organ nadzorczy ma osiem tygodni na reakcję. W ciągu miesiąca od wpływu wniosku o konsultacje, organ może przedłużyć termin konsultacji o sześć tygodni. Zakończenie konsultacji może przybrać formę: (1) braku działań ze strony organu, względnie poinformowania o prawidłowości, w sytuacji jeśli organ nie ma zastrzeżeń do zamierzonego przetwarzania i prawidłowości oceny, (2) pisemnego zalecenia oraz (3) dowolnego uprawnienia z wymienionych w art. 58 rozporządzenia w sytuacji gdy administrator niedostatecznie zidentyfikował lub zminimalizował ryzyko. Mogą to być w szczególności następujące działania naprawcze i doradcze: (1) wydanie ostrzeżenia administratorowi lub podmiotowi przetwarzającemu dotyczącego możliwości naruszenia przepisów rozporządzenia poprzez planowane operacje przetwarzania; (2) nakazanie administratorowi lub podmiotowi przetwarzającemu dostosowanie operacji przetwarzania do przepisów rozporządzenia, a w stosownych przypadkach wskazanie sposobu i terminu tego dostosowania; (3) wprowadzenie czasowego

lub całkowitego ograniczenia przetwarzania, w tym zakazu przetwarzania; (4) nałożenie administracyjnej kary pieniężnej zależnie od okoliczności konkretnej sprawy; (5) udzielenie administratorowi porady dotyczącej warunków przetwarzania.

Rozporządzenie daje także państwom członkowskim możliwość wprowadzenia obowiązku konsultacji i uzyskiwania od organu nadzorczego zgód na przetwarzanie danych do celów wykonania zadań realizowanych w interesie publicznym.

Możliwość przetwarzania danych osobowych wspólnie przez grupy kapitałowe, grupy przedsiębiorców w ramach współadministracji danymi osobowymi

Zakres podmiotowy nowych przepisów – co do zasady – nie zmienia definicji podstawowego adresata norm, tj. administratora danych. Należy jednak wyeksponować fakt, uzupełnienia katalogu o wprowadzaną przez RODO konstrukcję współadministratorów, wcześniej prawu nieznaną. Sednem współadministrowania jest realizacja jednego, bądź kilku celów przez więcej niż jednego administratora danych z wykorzystaniem tych samych zasobów jakimi są tożsame zestawy danych osobowych, będących w dyspozycji tych podmiotów[262].

Niezmiennie administratorem danych jest organ, jednostka organizacyjna, podmiot lub osoba decydująca o celach i środkach przetwarzania danych osobowych. W celu ustalenia, czy dany podmiot może być uznany za administratora danych, istotna jest przede wszystkim analiza przepisów dotyczących organizacji tego podmiotu w kontekście prowadzonego procesu przetwarzania danych osobowych. Dzięki temu można ustalić, kto decyduje o celach, dla których realizacji dane są przetwarzane, oraz kto dobiera środki służące do gromadzenia i dalszego wykorzystywania tych danych[263]. Trafną analizę w tym zakresie przeprowadzili Piotr Kowalik i Dariusz Wociór. „Przedsiębiorca jest administratorem danych osobowych wykorzystywanych w związku z prowadzącą przez siebie działalnością gospodarczą. Wykonywanie czynności administratora danych będzie u takiego przedsiębiorcy przypisane do konkretnej osoby lub grupy osób. O tym, kto to będzie, decyduje forma prawna działalności tego przedsiębiorcy oraz regulacje wewnętrzne u niego obowiązujące. W przypadku osób fizycznych prowadzących jednoosobową działalność gospodarczą to one same są administratorami danych osobowych gromadzonych w ramach tej działalności. Przetwarzanie danych osobowych u takich przedsiębiorców jest związane z aktywnością samego przedsiębiorcy – osoby fizycznej. Na samych takich przedsiębiorcach ciążą zatem wszystkie omówione w publikacji obowiązki administratora

[262] Ochrona praw i wolności osób, których dane dotyczą, oraz obowiązki i odpowiedzialność prawna, administratorów i podmiotów przetwarzających – także w odniesieniu do monitorowania ze strony organów nadzorczych i do środków przez nie stosowanych – wymagają dokonania w ramach rozporządzenia jasnego podziału obowiązków, także w sytuacji, gdy administrator określa cele i sposoby przetwarzania wspólnie z innymi administratorami lub gdy operacji przetwarzania dokonuje się w imieniu administratora. Motyw 79 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 (Dz. Urz. UE L 119 z dn. 4.05.2016, s. 1–88).

[263] Szerzej zob. 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.

danych osobowych. W związku z działalnością gospodarczą prowadzoną przez spółki prawa handlowego przyjmuje się, że administratorem danych osobowych są same spółki prawa handlowego. Administratorem danych jest sama spółka, a nie jej organy, osoby zasiadające w jej organach czy też pełniące w niej inne funkcje. Oczywiście w pewnych sytuacjach osoby te mogą ponosić odpowiedzialność za dane osobowe zgromadzone u tego przedsiębiorcy, jednak nie jako administrator danych, a co najwyżej jako osoby działające za niego lub w jego imieniu W przypadku spółek prawa handlowego, jak też i innych przedsiębiorców będących osobami prawnymi, czy też jednostkami organizacyjnymi nieposiadającymi osobowości prawnej, uznaje się, że wewnątrz ich struktury odpowiedzialne za realizację obowiązków administratora danych są osoby uprawnione do prowadzenia spraw tego przedsiębiorcy i jego reprezentację, względnie osoby zasiadające w organach tego przedsiębiorcy uprawnione do prowadzenia jego spraw i reprezentacji. Tym samym zarówno w przypadku spółek prawa handlowego, jak i innych przedsiębiorców w pierwszej kolejności należy zapoznać się z przepisami regulującymi działanie określonego podmiotu oraz regulacjami wewnętrznymi uszczegóławiającymi te przepisy. Pozwoli to ustalić, kto w danym podmiocie wykonuje czynności administratora danych osobowych"[264].

Wszędzie tam, gdzie obowiązki administratora danych wykonuje organ lub grupa wspólników, celowe jest wskazanie jednej osoby, która odpowiadałaby za obszar ochrony danych osobowych u tego przedsiębiorcy i realizację obowiązków administratora danych[265]. Sytuacja się prostuje wraz nowym rozwiązaniem prawnym zaproponowanym w rozporządzeniu, które wprowadza *novum* w postaci jednoznacznej możliwości wykonywania funkcji/roli administratora danych przez więcej niż jeden podmiot. „Współadministrowanie nie jest nową instytucją w prawie ochrony danych osobowych. Zgodnie z art. 2 lit. d dyrektywy 95/46 administrator danych oznaczał osobę fizyczną lub prawną, władzę publiczną, agencję lub inny organ, który samodzielnie lub wspólnie z innymi podmiotami określa cele i sposoby przetwarzania danych. Na kanwie przepisów dyrektywy, o byciu współadministratorem decydował będzie więc wyłącznie stan faktyczny – wspólnota celów i środków

[264] Zob. P. Kowalik, D. Wociór, *Administrator danych w sektorze przedsiębiorstw* [w:] *Ochrona danych osobowych i informacji niejawnych z uwzględnieniem ogólnego rozporządzenia unijnego*, red. D. Wociór, Warszawa 2016.

[265] W przypadku spółki jawnej, zgodnie z art. 39 k.s.h. każdy wspólnik ma prawo i obowiązek prowadzenia spraw spółki oraz każdy wspólnik może bez uprzedniej uchwały wspólników prowadzić sprawy nieprzekraczające zakresu zwykłych czynności spółki. W kontekście ochrony danych osobowych powoduje to, iż na wszystkich wspólnikach spółki jawnej ciążą obowiązki administratora danych. Powinni oni jednak wskazać spośród siebie jedną osobę odpowiedzialną za realizację tych zadań w spółce. Podobnie jest w przypadku spółki partnerskiej. Zgodnie z art. 89 k.s.h. w sprawach nieuregulowanych w k.s.h. dotyczącym tego rodzaju spółek – do spółki partnerskiej stosuje się odpowiednio przepisy o spółce jawnej, chyba że odrębna ustawa stanowi inaczej. Artykuł 97 k.s.h wskazuje, że umowa spółki partnerskiej może przewidywać, że prowadzenie spraw i reprezentowanie spółki powierza się zarządowi. Tym samym to umowa spółki wskazuje, czy do prowadzenia spraw spółki, czyli także realizacji obowiązków administratora danych, zobowiązani będą wspólnicy (partnerzy) czy też zarząd tej spółki. W spółce komandytowej bezpośrednio odpowiedzialni za wykonywanie funkcji administratora danych są komplementariusze jako wspólnicy uprawnieni do reprezentowania spółki i prowadzenia jej spraw. Tak samo w spółce komandytowo-akcyjnej obowiązki administratora danych osobowych wykonują komplementariusze. W spółce z ograniczoną odpowiedzialnością, która jest administratorem danych osobowych, za ochronę danych osobowych odpowiada zarząd. Zgodnie z art. 201, § 1 k.s.h. zarząd prowadzi sprawy spółki i reprezentuje spółkę. Także w spółce akcyjnej, która jest administratorem danych osobowych, to zarząd spółki odpowiada za ochronę danych osobowych. Zgodnie z art. 368, § 1 k.s.h. zarząd prowadzi sprawy spółki i reprezentuje spółkę. Tak jak w spółkach kapitałowych, w spółdzielni to zarząd spółdzielni jako jej organ odpowiada w imieniu administratora danych za ochronę danych osobowych i wykonywanie jego obowiązków. Wynika to z art. 48 Ustawy prawo spółdzielcze, zgodnie z którym zarząd kieruje działalnością spółdzielni oraz reprezentuje ją na zewnątrz. Z kolei w przypadku spółki cywilnej należy uznać, że każda ze stron takiej umowy jest administratorem danych przetwarzanych w związku z jej realizacją. Zob. ustawa z dnia 15 września 2000 r. Kodeks spółek handlowych (tj. Dz. U. z 2020 r. poz. 1526, 2320).

przetwarzania danych. Dyrektywa nie wymagała więc zawierania pomiędzy administratorami porozumienia, które determinowałoby status podmiotu jako współadministratora".

RODO wprowadza nowe definicje współadministratorów oraz grup przedsiębiorstw. Przepis art. 26 ust. 1 rozporządzenia ustala, iż jeżeli co najmniej dwóch administratorów wspólnie ustala cele i sposoby przetwarzania, są oni współadministratorami. W drodze wspólnych uzgodnień współadministratorzy w przejrzysty sposób określają odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z rozporządzenia, 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 RODO, chyba że przypadające im obowiązki i ich zakres określa prawo Unii lub prawo państwa członkowskiego, któremu administratorzy ci podlegają. W uzgodnieniach można wskazać punkt kontaktowy dla osób, których dane dotyczą. Grupa przedsiębiorstw oznacza zatem łączne występowanie co najmniej przedsiębiorstwa sprawującego kontrolę oraz przedsiębiorstwa przez nie kontrolowanego. Należy zauważyć, iż wcześniej również występowały sytuacje przetwarzania danych w ramach zespołu przedsiębiorców, czy w ramach grup kapitałowych, niemniej ówcześni administratorzy mieli te same prawa i obowiązki, a więc tak naprawdę każdy z nich był odrębnym administratorem.

Warto się zastanowić w jakich sytuacjach w praktyce może być wykorzystywana instytucja współadministrowania. Na pewno współadministrowanie najczęściej można spotkać w procesach przetwarzania w ramach grup kapitałowych np. w ramach prowadzenia rekrutacji, działań marketingowych. Innym przykładem może być sytuacja, w której dwie spółki są ze sobą ściśle powiązane organizacyjnie, kapitałowo i osobowo, a w ramach prowadzonej działalności gospodarczej wspólnie korzystają z jednej bazy danych klientów. Na poziomie szczegółowych sytuacji „współadministratorami w rozumieniu RODO, mogą być:

1) współorganizatorzy konkursów gdy oba podmioty pełnią funkcję organizatorów bądź fundatorów konkursów;
2) organy administracji wspólnie zarządzający systemem rejestrów państwowych;
3) adwokaci wspólnie reprezentujący klienta przed sądem;
4) biblioteki, które wspólnie kupują nowości wydawnicze zgodnie i przeprowadzają w tym celu wspólne badania opinii publicznej;
5) wspólnicy spółki cywilnej w ramach podejmowania przez nich większości wspólnych działań gdzie każdy ze wspólników ma status administratora danych osobowych;
6) kilku organizatorów koncertu w ramach monitoringu wizyjnego;
7) podmioty prowadzące wspólną bazę marketingową, ze wspólnym celem przetwarzania;
8) podmioty prowadzące wspólną rekrutację;
9) spółki celowe realizujące wspólne cele (np. tworzenie systemów informatycznych);

10) spółki z grupy kapitałowej prowadzące współdzieloną bazę CRM"[266].

Podobnie jak w przypadku określania, kto jest administratorem, a kto podmiotem przetwarzającym, dla ustalenia stosunku współadministrowania liczy się wyłącznie stan faktyczny i obiektywna ocena[267]. Oznacza to, że relacja współadministrowania istnieje niezależnie od tego, jak współpracujące podmioty opiszą łączące je stosunki np. w umowie. „Umowa o współadministrowanie nie musi stanowić odrębnego dokumentu. Może być częścią umowy głównej dotyczącej współpracy np. tworzenia wspólnych usług czy produktu. Umowa o współadministrowanie danymi osobowymi powinna co do zasady określać m.in.:

- po co i w jaki sposób dane osobowe będą przetwarzane,
- kto za co odpowiada w związku z przetwarzaniem danych osobowych,
- jak będą obsługiwane żądania podmiotów danych,
- kto będzie wypełniał obowiązki informacyjne względem podmiotów danych,
- jak dane osobowe będą zabezpieczane przez każdy z podmiotów,
- czy dopuszczalne będzie powierzenie przetwarzania danych osobowych,
- jak będzie wyglądała odpowiedzialność poszczególnych podmiotów"[268].

Kryteria pozwalające na uznanie, czy mamy w danym przypadku do czynienia ze współadministrowaniem danymi osobowymi, komplikuje nowe orzecznictwo Trybunału Sprawiedliwości Unii Europejskiej. Wydał on dwa ważkie orzeczenia, w których dokonał wykładni pojęcia współadministrowania. W wyroku z 5 czerwca 2018 roku, w sprawie C-210/16 TSUE[269] w składzie wielkiej izby uznał, iż podmiot prowadzący fanpage na Facebooku współadministruje danymi osobowymi razem z Facebookiem. Z kolei w wydanym 29 lipca 2019 roku wyroku w sprawie C-40/17 TSUE[270] uznał, że podmiot zamieszczający na swojej stronie internetowej ikonkę: „Lubię to" Facebooka, współadministruje danymi osobowymi łącznie z tym podmiotem[271]. Bez względu na to, czy uznaje się wyżej

[266] T. Osiej, *Współadministrowanie danymi osobowymi – co wiemy o tej instytucji?*, https://gdpr.pl/wspoladministrowanie-danymi-osobowymi-co-wiemy-o-tej-instytucji, [dostęp: 02.12.2020].

[267] Zob. I. Kowalczuk-Pakuła, M. Chołuj, *Współadministrowanie – nowy paradygmat w prawie ochrony danych osobowych*, Monitor Prawniczy – dodatek specjalny, Prawo nowych technologii 2019, nr 21, s. 16.

[268] Pełen wykaz elementów, które warto zawrzeć w uzgodnieniach między współadministratorami, obejmuje m.in.: (a) przedmiot współadministrowania, (b) cel, sposób, zakres przetwarzania danych, (c) kategoria osób, których dane osobowe będą przetwarzane, (d) okres przetwarzania danych osobowych, (e) podstawy i cele przetwarzania danych osobowych, (f) odpowiedzialność i podział zadań w zakresie naruszeń ochrony danych, (g) zasady współpracy w zakresie opracowywania oceny skutków dla ochrony danych, (h) zasady związane z powierzeniem danych osobowych oraz przekazywaniem danych osobowych do państw trzecich, (i) warunki w zakresie zabezpieczenia danych osobowych zgodnie z art. 24, 25 oraz 32 RODO, (j) szczegółowe określenie obowiązków współadministratorów w stosunku do osób, których dane dotyczą, w tym dotyczące spełnienia obowiązku informacyjnego, (k) informacja na temat tego, który ze współadministratorów zapewnia odpowiednie udokumentowanie w zakresie wykazania się zgodnością przetwarzania z RODO, (l) odpowiedzialność współadministratórow, (m) sposób kontaktów między współadministratorami. A. Rapcewicz, *Kilka słów o współadministrowaniu danymi osobowymi*, iSecure, https://www.isecure.pl/blog/kilka-slow-o-wspoladministrowaniu-danymi-osobowymi/, [dostęp: 02.12.2020]. Por. K. Kmiecicka, *Współadministrowanie danymi osobowymi*, https://blog-daneosobowe.pl/wspoladministrowanie-danymi-osobowymi/, [dostęp: 02.12.2020].

[269] Wyrok Trybunału Sprawiedliwości Unii Europejskiej z 5 czerwca 2018 roku (C-210/16), https://curia.europa.eu/juris/document/document.jsf;jsessionid=7C7F5AF47195D4A7611D87976D8765C4?text=&docid=202543&pageIndex=0&doclang=pl&mode=lst&dir=&occ=first&part=1&cid=8224414, [dostęp: 02.12.2020].

[270] Wyrok Trybunału Sprawiedliwości Unii Europejskiej z 29 lipca 2019 roku (C-40/17), https://curia.europa.eu/juris/document/document.jsf?text=&docid=216555&doclang=PL, [dostęp: 02.12.2020].

[271] Osią sporu pomiędzy niemiecką spółką Fashion ID GmbH & Co. KG, prowadzącą sprzedaż online artykułów odzieżowych, a Verbraucherzentrale NRW eV, czyli niemieckim stowarzyszeniem zajmującym się ochroną konsumentów, była zamieszczona na stronie internetowej Fashion ID wtyczka „Lubię to", której dostawcą jest portal społecznościowy Facebook Ireland. Niemieckie stowarzyszenie wniosło przeciwko Fashion ID powództwo o zaniechanie stosowania

przywołane orzeczenia w pełni za słuszne czy zbyt rygorystycznie, faktem jest że TSUE definiuje współadministrowanie nie tylko przez pryzmat sytuacji, gdy podmioty dokonują wszelkich ustaleń wspólnie w odniesieniu do celów i sposobów przetwarzania danych, lecz również wtedy, gdy oddzielne decyzje każdego z tych podmiotów łącznie kształtują proces przetwarzania danych w konkretnym przypadku. Takie rozumienie tej instytucji ma poważne konsekwencje prawne, w szczególności na poziomie odpowiedzialności deliktowej.

Rozporządzenie pozwala zatem podzielić się prawami i obowiązkami w ramach współadministracji, przy czym nie może się to odbywać ze szkodą dla osób, których dane są przetwarzane. Wprost reguluje to przepis art. 26 ust. 2 rozporządzenia. „Uzgodnienia, o których należycie odzwierciedlają odpowiednie zakresy obowiązków współadministratorów oraz relacje pomiędzy nimi a podmiotami, których dane dotyczą. Zasadnicza treść uzgodnień jest udostępniana podmiotom, których dane dotyczą"[272]. Grupa przedsiębiorstw może przykładowo wyznaczyć jednego Inspektora Ochrony Danych, o ile można będzie łatwo nawiązać z nim kontakt z każdej siedziby – co stanowi niewątpliwy handicap dla przedsiębiorców w stosunku do poprzednich rozwiązań. Podmioty będące współadministratorami, na podstawie poczynionych uzgodnień, mogą przekazywać sobie dane osobowe i nie potrzebują do tego żadnej dodatkowej podstawy prawnej. Odróżnia to współadministrowanie od przypadku udostępniania danych osobowych[273]. Bardzo ważne w praktyce jest również rozróżnienie pomiędzy rolą współadministratora, a podmiotu przetwarzającego. Ten drugi nie podejmuje żadnych decyzji co do celów i sposobów przetwarzania, zaś współadministrowanie to z definicji wspólne ustalanie celów. To warunek *sine qua non* powstania współadministrowania, w ramach którego nie dochodzi ani do udostępnienia danych, ani powierzenia.

Uzgodnienia mają chronić i gwarantować prawa podmiotów danych. Z drugiej strony – co istotne – niezależnie od uzgodnień w zakresie współadministrowania, zgodnie z art. 26 ust. 3 RODO, osoba której dane dotyczą, może wykonywać przysługujące jej prawa wynikające z rozporządzenia wobec każdego z współadministratorów. Oznacza

internetowej wtyczki, ponieważ korzystanie z niej prowadzi do naruszenia przepisów z zakresu ochrony danych osobowych. W toku postępowania dowodowego, prowadzonego przed niemieckim sądem, wykazano, że dzięki zamieszczeniu wtyczki „Lubię to" do Facebooka są przekazywane informacje o adresie IP oraz identyfikatorze przeglądarki osoby odwiedzającej witrynę Fashion ID, przy czym przekazanie tych danych następuje automatycznie po otwarciu strony internetowej Fashion ID oraz niezależnie od tego, czy osoba odwiedzająca stronę kliknęła przycisk „Lubię to", a nawet czy jest posiadaczem konta na Facebooku. Ustalono też, że Fashion ID nie ma żadnego wpływu ani na to, jaki zakres danych jest przekazywany do dostawcy wtyczki, ani na to, jakie działania podejmie dostawca wtyczki w związku z pozyskanymi danymi. W tym kontekście niemiecki sąd powziął wątpliwości dotyczące m.in. tego, czy w tak ukształtowanym procesie przetwarzania operator witryny internetowej pełni rolę administratora, a jeśli tak, to jakie wynikają z tego konsekwencje związane z koniecznością zapewnienia ochrony danych osobowych użytkowników. Odpowiadając na zadane pytania prejudycjalne, TS wskazał, że niewątpliwie Fashion ID pełni rolę administratora. A. Michałowicz, *Współadministrowanie danymi osobowymi. Konsekwencje wyroku Trybunału Sprawiedliwości w sprawie C-40/17 Fashion ID*,https://www.parp.gov.pl/component/content/article/63971:wspoladministrowanie-danymi-osobowymi-konsekwencje-wyroku-trybunalu-sprawiedliwosci-w-sprawie-c-40–17-fashion-id, [dostęp:02.12.2020].

[272] J. Byrski, H. Hoser, *Social media oraz technologie umożliwiające śledzenie użytkowników Internetu a współadministrowanie danymi osobowymi*, Monitor Prawniczy – dodatek specjalny, Prawo nowych technologii 2019, nr 21, s. 11.

[273] W przypadku udostępnienia dochodzi do przekazania danych osobowych przez jednego administratora innemu podmiotowi, który również staje się administratorem danych osobowych i będzie je przetwarzał we własnych celach. Aby mogło dojść do udostępnienia, po stronie administratora udostępniającego dane osobowe musi istnieć jedna z podstaw wskazanych w art. 6 ust. 1 lub art. 9 ust. 2 RODO (np. podmiot danych wyraził zgodę na udostępnienie danych innemu administratorowi albo przepis prawa zobowiązuje administratora do udostępnienia danych innemu administratorowi). Administrator – odbiorca również musi mieć podstawę prawną do przetwarzania danych osobowych na własne potrzeby. Zob. *Powierzenie przetwarzania danych a udostępnienie – różne formy przekazywania*, https://blog-daneosobowe.pl/powierzenie-a-udostepnienie-danych-rozne-formy-przekazywania/, [dostęp: 14.12.2021].

to, że podmiot danych, pomimo wskazania przez współadministratorów jednego punktu kontaktowego, nie jest tym ograniczony. W konsekwencji należy stwierdzić, że osoba której dane dotyczą nie jest związana uzgodnieniami współadministratorów (w zakresie realizacji praw).

Zgodnie z art. 82 ust. 4 rozporządzenia, wszyscy współadministratorzy odpowiadają solidarnie za szkodę wynikłą z naruszenia norm ochrony danych osobowych. Na mocy art. 82 ust. 5 RODO administrator, który zapłacił odszkodowanie ma prawo zwrotu części odszkodowania od pozostałych współadministratorów w części odpowiadającej części szkody, za którą ponoszą odpowiedzialność. Celem tej konstrukcji jest zapewnienie podmiotom danych realnego prawa do uzyskania odszkodowania.

Obowiązek wdrożenia i prowadzenia rejestru czynności przetwarzania danych względnie rejestru kategorii czynności przetwarzania

Rozporządzenie wprowadziło wymóg wdrożenia rejestru czynności związanych z przetwarzaniem danych jako swoistą rekompensatę za anulację obowiązku rejestrowania zbiorów danych. Zgodnie z motywem 82 RODO, wyróżniamy dwa podstawowe cele prowadzenia rejestrów: (a) zachowanie przez administratora i podmiot przetwarzający zgodności z przepisami RODO, za które są odpowiedzialni oraz (b) umożliwienie organowi nadzorczemu monitorowania wszystkich procesów przetwarzania danych w organizacji. Administrator lub podmiot przetwarzający oraz ich przedstawiciele mają obowiązek udostępnić rejestry na każde żądanie organu nadzorczego.

Rejestr czynności przetwarzania to dokument, w którym aktualizuje się informacje m.in. o tym, w jakich celach przetwarza się dane osobowe, kogo dotyczą te dane, jaki jest ich zakres, komu są ujawniane, do kiedy będą przechowywane. W rejestrze zamieszcza się także ogólne informacje o sposobie zabezpieczenia danych, a także o tym, czy są przekazywane poza Unię Europejską. Rozróżnia się dwa rejestry czynności przetwarzania – dla administratora danych osobowych (ten rejestr zawiera szerokie informacje o przetwarzanych danych) oraz dla podmiotu przetwarzającego (w tym rejestrze należy wskazać przede wszystkim, w imieniu jakich administratorów są przetwarzane dane osobowe, a także jaki jest zakres danych i rodzaj operacji, które są na nich wykonywane). Rejestry ułatwiają stałą weryfikację działalności w zakresie przetwarzania danych osobowych, systematyzują wykonywane czynności przetwarzania oraz pomagają w monitoringu prowadzonych operacji przetwarzania danych osobowych pod względem zgodności zarówno z wymaganiami prawnymi, jak i z celami biznesowymi. Informacje zebrane w rejestrach mogą posłużyć również administratorom i podmiotom przetwarzającym do oceny, czy powinni spełnić inne obowiązki wynikające z RODO, np. przeprowadzenie oceny skutków przetwarzania dla ochrony danych osobowych (jeśli podmiot przetwarza szczególne kategorie danych osobowych).

Obowiązek rejestrowania czynności przetwarzania obejmuje wszystkie operacje, jakie organizacja wykonuje na danych osobowych, takie jak zbieranie, organizowanie, przechowywanie, modyfikowanie, przeglądanie, wykorzystywanie, ujawnianie czy usuwanie. Trzeba mieć na uwadze, że dana jednostka organizacyjna może być dysponentem procesów, które realizuje zarówno:

1) we własnym imieniu – wtedy jako administrator prowadzi rejestr czynności przetwarzania (art. 30 ust. 1 RODO),
2) wspólnie z innymi – jako jeden ze współadministratorów – wtedy jako administrator prowadzi rejestr czynności przetwarzania (art. 30 ust. 1 RODO),
3) w imieniu innych organizacji – wtedy jako podmiot przetwarzający prowadzi rejestr wszystkich kategorii czynności przetwarzania (art. 30 ust. 2 RODO).

Rozporządzenie wyróżnia zatem dwa rodzaje rejestrów: (1) czynności przetwarzania, oraz (2) kategorii czynności przetwarzania. Do prowadzenia pierwszego zobowiązani są administratorzy danych. Obowiązek prowadzenia rejestru czynności przetwarzania spoczywa na każdym administratorze danych, który nie przetwarza danych osobowych w sposób „sporadyczny"[274]. Zgodnie z art. 30 ust. 5 rozporządzenia obowiązek prowadzania rejestru czynności i rejestru kategorii czynności nie ma zastosowania do przedsiębiorcy lub podmiotu zatrudniającego mniej niż 250 osób, chyba że czynności przetwarzania, które wykonują: (1) mogą powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą; (2) nie mają charakteru sporadycznego lub obejmują szczególne kategorie danych osobowych, o których mowa w art. 9 ust. 1 RODO, lub (3) dotyczą wyroków skazujących i naruszeń prawa, o czym mowa w art. 10 RODO[275].

Artykuł 30 rozporządzenia stanowi, iż każdy administrator oraz – gdy ma to zastosowanie – przedstawiciel administratora prowadzą rejestr czynności przetwarzania danych osobowych, za które odpowiadają. W rejestrze zamieszcza się następujące informacje:

- imię i nazwisko lub nazwa oraz dane kontaktowe administratora, współadministratorów i Inspektora Danych Osobowych,
- cele przetwarzania danych osobowych,
- opis kategorii osób, których dane dotyczą oraz kategorii danych osobowych,
- kategorie odbiorców, którym zostały udostępnione dane osobowe (lub będą udostępnione w przyszłości), w tym odbiorców w państwach trzecich i w międzynarodowych organizacjach,

[274] Zob. *Rejestrowanie czynności przetwarzania*, Poradnik Prezesa UODO, https://uodo.gov.pl/pl/123/214, [dostęp: 27.11.2020].

[275] W motywie 13 preambuły RODO wskazano, że wyjątek dotyczący rejestrowania czynności przetwarzania dla podmiotów zatrudniających mniej niż 250 pracowników przewidziano ze względu na szczególną sytuację mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw. W związku z licznymi pytaniami dotyczącymi stosowania tego wyłączenia od obowiązku prowadzenia rejestru czynności i rejestru kategorii czynności Grupa Robocza Art. 29 (Europejska Rada Ochrony Danych – EROD), w pracach której uczestniczy Prezes Urzędu Ochrony Danych Osobowych, opublikowała swoje stanowisko. la jego powstania wystarczy, że zachodzi którakolwiek z tych sytuacji samodzielnie. Rejestr czynności przetwarzania trzeba jednak prowadzić jedynie dla tych, wskazanych rodzajów przetwarzania. Jako przykład Grupa Robocza Art. 29 podaje przypadek małej organizacji, która najprawdopodobniej systematycznie przetwarza dane dotyczące swoich pracowników. Jak wskazuje „w rezultacie takie przetwarzanie nie może być uznane za „sporadyczne" i musi w związku z tym być zawarte w rejestrze czynności przetwarzania. Zob. 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.

- informacje na temat przekazania danych osobowych do państw trzecich (z podaniem nazwy państwa) lub organizacji międzynarodowych (z podaniem nazwy organizacji), a w przypadku przekazań — dokumentacja odpowiednich zabezpieczeń,
- planowane terminy usunięcia poszczególnych kategorii danych osobowych,
- opis technicznych i organizacyjnych środków bezpieczeństwa zastosowanych wobec przetwarzanych danych osobowych.

Obowiązek prowadzenia rejestrów w określonych przypadkach spoczywa też na przedstawicielach administratora i podmioty przetwarzające (procesorzy). Zgodnie z rozporządzeniem obowiązek wyznaczenia swojego przedstawiciela mają administrator i podmiot przetwarzający nieposiadający jednostek organizacyjnych w Unii wówczas, jeżeli prowadzone przez nich 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 monitorowaniem ich zachowania, o ile do zachowania tego dochodzi w Unii[276]. W przypadku współadministratorów i procesów przetwarzania danych, w zakresie których wspólnie ustalane są cele i sposoby przetwarzania danych, przyjąć należy, że obowiązek prowadzenia rejestru ciąży na każdym z nich. Wskazuje na to zarówno brzmienie art. 30 ust. 1 rozporządzenia, zgodnie z którym do prowadzenia rejestru zobowiązany jest „każdy" administrator danych, a ponadto cel tego obowiązku, jakim jest zapewnienie – zarówno przez administratora, jak i przez organ nadzorczy – zgodności z RODO. W takim przypadku w rejestrze każdego ze współadministatorów powinien się znaleźć opis procesów przetwarzania objętych współadministrowaniem.

Zgodnie z art. 30 ust. 2 rozporządzenia, każdy podmiot przetwarzający dane (procesor) ma obowiązek prowadzenia rejestru kategorii czynności przetwarzania. Podmiot przetwarzający dane przetwarza je w imieniu administratora. W takim rejestrze zamieszcza się, co najmniej, następujące informacje:

- imię i nazwisko lub nazwa oraz dane kontaktowe podmiotu przetwarzającego lub podmiotów przetwarzających oraz każdego administratora, w imieniu którego działa podmiot przetwarzający, a gdy ma to zastosowanie – przedstawiciela administratora lub podmiotu przetwarzającego oraz Inspektora Ochrony Danych,
- kategorie przetwarzań dokonywanych w imieniu każdego z administratorów,
- informacje na temat przekazania danych osobowych do państwa trzeciego (z podaniem nazwy państwa) lub organizacji międzynarodowej (z podaniem nazwy organizacji), a w przypadku przekazań – dokumentacja odpowiednich zabezpieczeń,
- opis technicznych i organizacyjnych środków bezpieczeństwa zastosowanych wobec przetwarzanych danych osobowych.

[276] Zob. art. 27 w zw. z art. 3 ust. 2 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 (Dz. Urz. UE L 119 z dn. 4.05.2016, s. 1–88).

W odróżnieniu od rejestru czynności – rejestr kategorii czynności nie obejmuje celów przetwarzania, opisu kategorii osób, których dane dotyczą, kategorii danych osobowych oraz kategorii odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych[277]. Tak jak rejestr czynności, tak i rejestr kategorii czynności może obejmować inne elementy niż wskazane w art. 30 ust. 2 RODO, w szczególności takie, które podmiot przetwarzający uznaje za potrzebne i uzasadnione dla zapewnienia zgodności z prawem przetwarzania danych, które zostało mu powierzone. Fakultatywnymi elementami rejestru mogą być następujące przykładowe elementy:

- wskazanie użytego do przetwarzania systemu informatycznego,
- czas trwania umowy (ze wskazaniem daty),
- dane kontaktowe podmiotów, którym powierzono dane osobowe.

Zarówno rejestr czynności przetwarzania, jak i rejestr kategorii czynności przetwarzania mogą być wzbogacane o inne elementy, które zostaną uznane za zasadne (z uwagi na specyfikę administratora lub podmiotu przetwarzającego), takie jak: (a) wskazanie podstawy prawnej przetwarzania, (b) wskazanie źródła pozyskania danych, (c) wskazanie użytego do przetwarzania systemu informatycznego, (d) informacje dotyczące przeprowadzonej oceny skutków dla ochrony danych. Niekiedy uzasadnione może okazać się uwzględnienie w rejestrze również informacji na temat: (a) tzw. właścicieli procesów, czyli osób odpowiedzialnych u administratora za konkretne czynności przetwarzania, czy (b) danych kontaktowych podmiotu przetwarzającego oraz podmiotów, którym powierzono wykonywanie określonych czynności przetwarzania danych lub określonych operacji w ramach tych czynności (art. 28 ust. 4 RODO).

Nie można pominąć faktu, iż Prezes Urzędu Ochrony Danych Osobowych przygotował gotowe szablony rejestru czynności przetwarzania i rejestru kategorii czynności wraz z przykładami ich uzupełnienia oraz wyjaśnienia, które to dotyczą sposobu realizacji obowiązku prowadzenia rejestrów[278].

Wzory rejestrów Prezesa Urzędu nie są po pierwsze jedynymi prawidłowymi wzorami, po drugie z oczywistych względów powinny być dopasowane do charakterystyki administratora (każda jednostka organizacyjna jest inna). Stąd ze względu na różnorodność administratorów, sektorów w których działają i procesów przetwarzania danych, które prowadzą, zakłada się, iż w praktyce może występować wiele różnych wzorów rejestru czynności. Istotne jest aby w każdym przypadku administrator lub podmiot przetwarzający był w stanie, w sposób czytelny i przejrzysty, przedstawić wymagane na mocy art. 30 ust. 1 i 2 RODO, elementy

[277] Określenie tych okoliczności jest obowiązkiem administratora lub współadministratora jako podmiotów, które zgodnie z definicją zawartą w art. 4 pkt 7 RODO decydują o celach i sposobach przetwarzania danych, chyba że cele te i sposoby określone są w przepisach prawa, na podstawie których działa administrator lub współadministrator. Szerzej zob. *Jak wypełnić rejestr kategorii czynności przetwarzania danych*, https://www.poradyodo.pl/aktualnosci-rodo/jak-wypelnic-rejestr-kategorii-czynnosci-przetwarzania-danych-9231.html, [dostęp: 27.11.2020].

[278] *Rejestrowanie czynności przetwarzania*, Poradnik Prezesa UODO, https://uodo.gov.pl/pl/123/214, [dostęp: 27.11.2020].

RYSUNEK 11 Rejestr czynności przetwarzania na przykładzie szkoły (wzór PUODO)

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
L.P.	**Nazwa czynności przetwarzania**	**Jednostka organizacyjna (department, dział itp.)**	**Cel przetwarzania**	**Kategorie osób**	**Kategorie danych**	**Podstawa prawna**	**Źródło danych**	**Planowany termin usunięcia kategorii danych** *(jeśli jest to możliwe)*	**Nazwa współadministratora i dane kontaktowe** *(jeśli dotyczy)*	**Nazwa podmiotu przetwarzającego i dane kontaktowe** *(jeśli dotyczy)*	**Kategorie odbiorców** *(innych niż podmiot przetwarzający)*	**Nazwa systemu lub oprogramowania**	**Opis z opis techniczny i organizacyjnych środków bezpieczeństwa zgodnie z art. 32 ust. 1** *(jeżeli jest to możliwe)*	**DPIA** **(jeśli tak, lokalizacja raportu)**	**Transfer do kraju trzeciego lub organizacji międzynarodowej (nazwa kraju i podmiotu)**	**Jeśli transfer i art. 49 ust. 1 akapit drugi - dokumentacja odpowiednich zabezpieczeń**
			Art.. 30 ust. 1 pkt b	**Art.. 30 ust. 1 pkt c**	**Art.. 30 ust. 1 pkt c**			**Art.. 30 ust. 1 pkt f**	**Art.. 30 ust. 1 pkt a**	**Art.. 30 ust. 1 pkt d**	**Art.. 30 ust. 1 pkt d**		**Art.. 30 ust. 1 pkt g**		**Art. 30 ust. 1 pkt e**	**Art. 30 ust. 1 pkt e**
1.	**Rekrutacja pracowników pomocniczych, administracyjnych oraz nauczycieli**	**Dyrektor Szkoły**	**Rekrutacja pracowników**	**Kandydaci do pracy**	**Dane identyfikacyjne, dane adresowe, dane o wykształceniu, stażu pracy, uprawnieniach zawodowych, informacja z Krajowego Rejestru Karnego w przypadku nauczycieli**	**• Czynności zmierzające do zawarcia umowy w zw. z art. 22[1] § 1 ustawy z dnia 26 czerwca 1974 r. Kodeks Pracy (Dz. U. z 2018 r., poz. 108 t.j.);** **• Zgoda osób, których dane dotyczą - zakres wykraczający poza wskazany w art. 22[1] § 1**	**Kandydaci do pracy**	**Po zakończeniu procesu rekrutacyjnego**	**Nie dotyczy**	**Nie dotyczy**	**Dane nie są przekazywane innym podmiotom**	**System Kadry. Dokumentacja papierowa.**	**Zamykane szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola dostępu do systemu informatycznego, dostęp tylko dla osób upoważnionych.**	**Po przeprowadzeniu oceny ryzyka podjęto decyzję, że ocena skutków dla ochrony danych nie jest wymagana.**	**Nie dotyczy**	**Nie dotyczy**
2.	**Prowadzenie rejestru pracowników, akt pracowniczych i ewidencji czasu ich pracy**	**Samodzielne stanowisko ds. kadr**	**Prowadzenie ewidencji pracowników zgodnie z Kodeksem Pracy**	**Pracownicy pomocniczy (recepcjonistki, sprzątaczki), pracownicy gospodarczy), administracyjni**	**Dane identyfikacyjne, dane adresowe, dane o wykształceniu, przebiegu pracy, absencji (urlopy, zwolnienia lekarskie, rehabilitacyjne,zakolenie we inne), dane o zakresie**	**• Umowa o pracę.** **• Przepis prawa. Ustawa z dnia 26 czerwca 1974 r. Kodeks Pracy (Dz. U. z 2018 r., poz. 108 t.j.) - w szczeg. art. 22[1] w związku z art. 94 pkt 9a i 9b**	**Pracownik**	**50 lat [art. 51u ust 1 ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz. U. z 2018 r., poz. 217**	**Nie dotyczy**	**Nie dotyczy**	**ZUS, inne firmy ubezpieczeniowe - dotyczy tylko osób posiadających polisy ubezpieczeniowe**	**System Kadry. Dokumentacja papierowa.**	**Zamykane szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola dostępu do systemu informatycznego, dostęp tylko dla upoważnionych osób.**	**Po przeprowadzeniu oceny ryzyka podjęto decyzję, że ocena skutków dla ochrony danych nie jest wymagana.**	**Nie dotyczy**	**Nie dotyczy**
3.	**Zgłoszenie pracowników i członków ich rodzin do ZUS, ich aktualizacja i przekazywanie danych o zwolnieniach.**	**Samodzielne stanowisko ds. kadr**	**Zgłoszenia pracownika i członków jego rodziny do ZUS, ich aktualizacja oraz przekazywanie informacji o zwolnieniach.**	**Pracownicy pomocniczy (recepcjonistki, sprzątaczki, pracownicy gospodarczy), administracyjni oraz nauczyciele**	**Dane identyfikacyjne, dane adresowe, dane o Odziale NFZ oraz inne dane wymagane w formularzu zgłoszenia ZUS ZUA - zgłoszenie, ZUS IUA - zmiana danych, ZUS ZWUA -wyrejestrowanie, ZUS ZCNA -zgłoszenie członka rodziny, ZAS - wniosek o ustalenie okresu**	**• Przepis prawa. Ustawa z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych (Dz.U. z 2017 r., poz. 1778 t.j.) - art. 1, 6 oraz 6a**	**Pracownik**	**50 lat [art. 125a ust 4 ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych (Dz.U. z 2017 r., poz. 1778 t.j.) - art. 1, 6 oraz 6a** **50 lat [art. 125a ust 4 ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych (Dz.U.z 2017 r., poz.1383)]**	**Nie dotyczy**	**Nie dotyczy**	**ZUS, inne firmy ubezpieczeniowe - dotyczy tylko osób posiadających polisy ubezpieczeniowe**	**Systemy Kadry. Płatnik. Dokumentacja papierowa.**	**Zamykane szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola dostępu do systemu informatycznego, dostęp tylko dla upoważnionych osób, instalacja oprogramowania zabezpieczającego typu firewall, system antywirusowy, system wykrywania włamań.**	**Po przeprowadzeniu oceny ryzyka podjęto decyzję, że ocena skutków dla ochrony danych nie jest wymagana.**	**Nie dotyczy**	**Nie dotyczy**
4.	**Prowadzenie rozliczeń z pracownikami, wypłata wynagrodzeń naliczanie obciążeń oraz naliczanie składek do ZUS**	**Samodzielne stanowisko ds. płac**	**Prowadzenie rozliczeń z pracownikami, naliczanie potrąceń, obliczanie składek ZUS**	**Pracownicy pomocniczy (recepcjonistki, sprzątaczki, pracownicy gospodarczy), administracyjni oraz nauczyciele**	**Dane identyfikacyjne, dane adresowe, dane kadrowe (wysługa lat pracy, stawka wynagrodzeń), dane o czasie pracy, przyznanych nagrodach, potrąceniach (składki związkowe, zajęcia komornicze itp.) numery kont dla przelewów bankowych pracownika**	**Umowa o pracę. Przepis prawa.** **• Ustawa z dnia 26 czerwca 1974 r. Kodeks Pracy (Dz. U. z 2018 r., poz. 108 t.j.) Dział III - Wynagrodzenia; ustawa z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych (Dz.U. z 2017 r., poz. 1778 t.j.) - art. 1, 6**	**Pracownik**	**50 lat [art. 125a ust 4 ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych (Dz.U.z 2017 r., poz.1383)]**	**Nie dotyczy**	**Nie dotyczy**	**Banki, urzędy skarbowe, ZUS, inne firmy ubezpieczeniowe - dotyczy tylko osób posiadających polisy ubezpieczeniowe,**	**System Place. Płatnik. Dokumentacja papierowa.**	**Zamykane szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola dostępu do systemu informatycznego, dostęp tylko dla upoważnionych osób, instalacja oprogramowania zabezpieczającego typu firewall, system antywirusowy, system wykrywania włamań.**	**Po przeprowadzeniu oceny ryzyka podjęto decyzję, że ocena skutków dla ochrony danych nie jest wymagana.**	**Nie dotyczy**	**Nie dotyczy**
5.	**Rekrutacja uczniów do szkół podstawowych**	**Dyrektor Szkoły**	**Przeprowadzenie rekrutacji do szkoły podstawowej**	**Kandydaci, rodzice, opiekunowie prawni**	**Imię, nazwisko, datę urodzenia oraz numer PESEL kandydata, a w przypadku braku numeru PESEL - serię i numer paszportu lub innego dokumentu potwierdzającego tożsamość; adres poczty elektronicznej i numery telefonów rodziców kandydata , oświadczenie o miejscu zamieszkania rodziców kandydata i kandydata, oświadczenie o wielodzietności rodziny kandydata,orzeczenie o potrzebie kształcenia specjalnego wydane ze względu na**	**Przepis prawa.** **• Ustawa z dnia 14 grudnia 2016 r. Prawo oświatowe (Dz.U. z 2017 r., poz., 59) , w szczególności art. 133**	**Zgłoszenie dokonane przez rodziców lub opiekunów prawnych**	**1 rok [art. 160 ust. 2 ustawy z 14 grudnia 2016 r. Prawo oświatowe (Dz.U. z 2017 r., poz. 59)]**	**organ prowadzący (prezydent, burmistrz, wójt)**	**Nie dotyczy**	**Dane nie są przekazywane innym podmiotom**	**Elektroniczny system rekrutacji. Dokumentacja papierowa.**	**Zamykane szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola dostępu do systemu informatycznego, dostęp tylko dla upoważnionych osób, instalacja oprogramowania zabezpieczającego typu firewall, system antywirusowy, system wykrywania włamań. Szyfrowana transmisja podczas przekazywania danych**	**Po przeprowadzeniu oceny ryzyka podjęto decyzję, że ocena skutków dla ochrony danych nie jest wymagana.**	**Nie dotyczy**	**Nie dotyczy**
6	**Ewidencja uczniów**	**Sekretariat Szkoły**	**Prowadzenie księgi uczniów**	**Uczniowie szkoły**	**Dane identyfikacyjne ucznia (imię, nazwisko,data i miejsce urodzenia, numer PESEL),** **Adres zamieszkania ucznia,** **Dane o rodzicach (imię, nazwisko adres zamieszkania - jeżeli są różne od adresu zamieszkania ucznia,** **Datę rozpoczęcia nauki, oddział do którego przyjęto oraz datę ukończenia szkoły albo datęi przyczynę jej opuszczenia.**	**Przepis prawa** **Ustawa z dnia 7 września 1991 r. o systemie oświaty (Dz. U. 2017, poz. 2198)** **§ 6 Rozporządzenia Ministra Edukacji Narodowej z dnia 29 sierpnia 2014 r. w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji przebiegu nauczania,**	**Rodzice uczniów, opiekunowie prawni.** **Dane otrzymane z gminy o osobach podlagających obowiązkowi szkolnemu.**	**10 lat**	**Nie dotyczy**	**Firma XYZ z siedzibą we Wrocławiu przy ul. Xyz 15.** **Zakres powierzenia obejmuje udostępnienie poprzez sieć internet Systemu Szkła Net - modul Sekretariat wraz z usługą zapewnienia ciągłości działania, konfiguracją zabezpieczeń oraz zapewnieniem kobpp bezpieczeństwa**	**Dane są przekazywane do Systemu Informacji Oświatowej na podstawie art. 14 Ustawy z dnia 15 kwietnia 2011 r. o Systemie Informacji Oświatowej Dz. U. 2017, poz. 2159)**	**System SzkolaNet, modul Sekretariat**	**Ścisle kontrolowany dostęp do danych - dostęp tylko dla uprawnionych, zarejestrowanych użytkowników.** **Komputery używane do dostępu do danych zabezpieczono przed atakami z sieci zewnętrznej systemem antywirusowym.** **Transmisja danych do oraz z serwera bazy danych systemu zabezpieczona jest kryptograficznie.** **Serwer i dostęp do baz danych zabezpieczony jest przez dostawcę usługi na poziomie**	**Z uwagi na powierzenie danych osobowych dzieci podmiotowi zewnętrznemu, przeprowadzono ocenę ryzyka nieuprawnionego dostępu do danych.** **Analiza wykazała, że zabezpieczenie zastosowane przez dostawcę usługi nie stwarzają dużego ryzyka nieuprawnionego dostępu do danych. Szczegóły dostępne są w raporcie podsumowującym wyniki oceny skutków dla czynności prowadzenia**	**Nie dotyczy**	**Nie dotyczy**
7	**Prowadzenie dziennika lekcyjnego**	**Nauczyciele, Wychowawca klasy**	**Rejestracja tematyów zajęć i wyników nauczania**	**Uczniowie szkoły, Rodzice, Nauczyciele**	**Dane identyfikacyjne ucznia (nazwisko, imiona, data i miejsce urodzenia)** **Adres zamieszkania,** **Dane o rodzicach (imię, nazwisko adres zamieszkania, adresy poczty elektronicznej, numery telefonów).** **Imiona i nazwiska nauczycieli prowadzących zajęcia, tygodniowy plan zajęć)** **Tematy zajęć i obecności, nieobecności (usprawiedliwione i**	**Przepis prawa.** **• Ustawa z dnia 7 września 1991 r. o systemie oświaty (Dz. U. 2017, poz. 2198)** **• § 10 Rozporządzenia Ministra Edukacji Narodowej w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji (Dz. U. z 2014 r. poz. 1170)**	**Uprawnieni nauczyciele, uprawnieni rodzice.**	**10 lat**	**Nie dotyczy**	**Firma XYZ z siedzibą we Wrocławiu przy ul. Xyz 15.** **Zakres powierzenia obejmuje udostępnienie poprzez sieć internet Systemu Szkła Net - modul Sekretariat wraz z usługą zapewnienia ciągłości działania, konfiguracją zabezpieczeń oraz zapewnienie kopii bezpieczeństwa**	**Dane są przekazywane wyłącznie uprawnionym rodzicom.**	**System SzkolaNet, modul Dziennik elektroniczny**	**Ścisle kontrolowany dostęp do danych - dostęp tylko dla uprawnionych, zarejestrowanych użytkowników.** **Transmisja danych do oraz z serwera bazy danych systemu zabezpieczona jest kryptograficznie.** **Serwer i dostęp do baz danych zabezpieczony jest przez dostawcę usługi wdrożeniem środków ochrony fizycznej i logicznej poprzez zastosowanie firewall i innych narzędzi zabezpieczających.**	**Z uwagi na powierzenie danych osobowych dzieci podmiotowi zewnętrznemu, przeprowadzono ocenę ryzyka nieuprawnionego dostępu do danych.** **Analiza wykazała, że zabezpieczenie zastosowane przez dostawcę usługi nie stwarzają dużego ryzyka nieuprawnionego dostępu do danych. Szczegóły dostępne są w raporcie podsumowującym wyniki oceny skutków dla czynności prowadzenia ewidencji uczniów.**	**Nie dotyczy**	**Nie dotyczy**

Źródło: *Rejestrowanie czynności przetwarzania. Poradnik Prezesa UODO*, https://uodo.gov.pl/pl/123/214, [dostęp: 27.11.2020]

RYSUNEK 12 Rejestr kategorii czynności przetwarzania – e-commerce (wzór PUODO)

	1	2	3	4	5	6	7	8	9	10	11
0	Kategorie przetwarzań	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa (jeżeli jest to możliwe)	Administrator				Czas trwania przetwarzania	Nazwy państw trzecich lub organizacji międzynarodowych, do których dane są przekazywane	Dokumentacja odpowiednich zabezpieczeń danych osobowych przekazywanych na podstawie art. 49 ust. 1 akapit drugi	Podprzetwarzający (podwykonawca) - jeśli dotyczy	
			Nazwa i dane kontaktowe administratora	Nazwa i dane kontaktowe współadministratora (jeśli dotyczy)	Nazwa i dane kontaktowe przedstawiciela administratora (jeśli [illegible])	Inspektor ochrony danych administratora (jeśli powołano)				Nazwa i dane kontaktowe podprzetwarzającego (podwykonawcy)	Kategorie podpowierzonych przetwarzań
	Art. 30 ust. 2 lit. b	Art. 30 ust. 2 lit. d, art. 32 ust. 1	Art. 30 ust. 2 lit. a					Art. 30 ust. 2 lit. c	Art. 30 ust. 2 lit. c		
1	Udostępnienie i utrzymywanie zdalnej platformy programistycznej do prowadzenia sklepu internetowego w środowisku sprzętowo-programowym wynajętym przez przetwarzającego	• Kontrola dostępu do infrastruktury, aplikacji i baz danych. • Dostęp do danych otrzymują wyłącznie osoby wskazane przez przetwarzającego na zlecenie administratora (czynności związane z modyfikacją funckjonalności, konserwacyjne, naprawcze). • Szyfrowana transmisja danych.	**Spółka BCA - sklep www** ul. Kwiatkowa 5 kontakt@bcaspolka.pl tel.: 123 456 789	**Nie dotyczy**	**Nie dotyczy**	**Andrzej Nowak** jan@bcaspolka.pl tel.: 123 456 788	**29 marca 2019 r**	**Szwajcaria** (przetwarzający w celu realizacji tej usługi korzysta z usług podwykonawcy w Szwajcarii)	**Nie dotyczy**	**Beispiel Rechenzentrum A.B.C GmbH** ul. Beispiel Straße 123/3 3006 Berno, Szwajcaria info@beispielrechencetrum.ch	**Przechowywanie, udostępnianie, utrwalanie i usuwanie danych w ramach udostępnianiej mocy obliczeniowej procesorów, przestrzeni pamięci operacyjnej i dyskowej.**
2			**Sklep Internetowy XYZ** ul. DanychOosobowych 1, tel.: 123 545 567, kontakt@sklepxyz.pl	**Nie dotyczy**	**Andrzej Przykładowy** andrzej@sklepintxyz.pl tel.: 999 444 321	**Jan Bezpieczny** jan@sklepintxyz.pl tel.: 123 456 788	**29 marca 2019 r.**				
3			**PrzykładowySklep.pl** ul. Przykładowa 4/5 tel. 765 432 234 kontakt@przykladowysklep.pl	**Nie dotyczy**	**Nie dotyczy**	**Imię Nazwisko** imie@sklep.pl tel.: 333 444 555	**22 maja 2021 r.**				
4			**Spółka ABC** ul. IOD 5 kontakt@spolkaabc.pl tel.: 133 456 888	**Nie dotyczy**	**Nie dotyczy**	**Imię Nazwisko** iod@spolkaabc.pl tel.: 123 456 788	**23 maja 2020 r.**				
5	**Udostępnienie i utrzymywanie zdalnej platformy programistycznej do prowadzenia rekrutacji pracowników w środowisku sprzętowo-programowym wynajętym przez przetwarzającego**	• Kontrola dostępu do infrastruktury, aplikacji i baz danych. • Dostęp do danych otrzymują wyłącznie osoby wskazane przez przetwarzającego na zlecenie administratora (czynności związane z modyfikacją funckjonalności, konserwacyjne, naprawcze). • Szyfrowana transmisja danych.	**Agencja Pracy XYZ** ul. Przykładowa 35/3 00-950 Warszawa kontakt@przedsiebiorstwekrutacyjnea.pl tel.: 133 456 888	**Agencja pracy ABC** ul. Przykładowa 5/2 00-950 Warszawa kontakt@agencja.pl tel.: 133 456 888	**Jan Headhunter** JanH@agencjaabc.pl tel.: 444 565 321	**Imię Nazwisko** iod@agencjaabc.pl tel.: 123 456 788	**29 marca 2019 r.**	**Nie dotyczy**	**Nie dotyczy**	**G.H.C. Centre de données exemplaire** ul. Exemple De Rue 3/4 13012 Marsylia, Francja info@centrededonneesexample.fr	**Przechowywanie, udostępnianie, utrwalanie i usuwanie danych w ramach udostępnianiej mocy obliczeniowej procesorów, przestrzeni pamięci operacyjnej i dyskowej.**
6	**Dostarczenie usługi wsparcia technicznego (instalacji, konfiguracji, naprawy, odzyskania po awarii, przygotowania raportów z bazy danych itp.) dla systemu Kadry-Place-ABZ w środowisku sprzętowo-programowym administratora**	• Kontrola dostępu do aplikacji i baz danych. • Dostęp do danych otrzymują wyłącznie osoby wskazane przez administratora systemu. • Szyfrowana transmisja danych podczas prac konserwacyjnych i naprawczych.	**Biuro rachunkowe Palma ABC** ul. Pod palmą 1/3 00-950 Warszawa kontakt@BiuroPalma.pl	**Nie dotyczy**	**Nie dotyczy**	**Wiktor Rokita** iod@BiuroPalma.pl tel.: 444 452 632	**30 grudnia 2020 r.**	**Nie dotyczy**	**Nie dotyczy**	**Nie dotyczy** **(dane przetwarzane są w prywatnej infrastrukturze przetwarzającego)**	**Nie dotyczy**
7			**Biuro rachunkowe XYZ** ul. XYZ/3 00-950 Warszawa kontakt@Biurorachunkowe.pl tel.: 133 456 334	**Nie dotyczy**	**Nie dotyczy**	**Jan Radler** JanR@BiurorachXYZ.pl tel.: 444 452 321	**30 grudnia 2020 r.**	**Nie dotyczy**	**Nie dotyczy**	**Nie dotyczy** **(dane przetwarzane są w prywatnej infrastrukturze przetwarzającego)**	**Nie dotyczy**
8	**Udostępnienie i utrzymywanie zdalnej platformy programistycznej do prowadzenia dziennika lekcyjnego w środowisku sprzętowo-programowym przetwarzającego**	• Kontrola dostępu do infrastruktury, aplikacji i baz danych. • Dostęp do danych otrzymują wyłącznie osoby wskazane przez przetwarzającego na zlecenie administratora (czynności związane z modyfikacją funckjonalności, konserwacyjne, naprawcze). • Szyfrowana transmisja danych.	**Szkoła Podstawowa nr X w Warszawie** ul. Przykładowa 4 sekretaria@szkola23.pl tel.: 12 345 678 333	**Nie dotyczy**	**Nie dotyczy**	**Imię Nazwisko** iod@szkola23.pl tel.: 123 456 788	**24 czerwca 2020 r.**	**Nie dotyczy**	**Nie dotyczy**	**Nie dotyczy** **(dane przetwarzane są w prywatnej infrastrukturze przetwarzającego)**	**Nie dotyczy**
9			**Liceum Ogólnokształcące nr Y w Warszawie** ul. Przykładowa 3/3 sekretariat@liceumogolnokształcacey.pl tel. 12 345 678 987	**Nie dotyczy**	**Nie dotyczy**	**Imię Nazwisko** iod@LOnrY.edu.pl tel.: 123 456 788	**22 czerwca 2021 r.**	**Nie dotyczy**	**Nie dotyczy**	**Nie dotyczy** **(dane przetwarzane są w prywatnej infrastrukturze przetwarzającego)**	**Nie dotyczy**
10	**Dostarczenie licencji systemu do prowadzenia dziennika elektronicznego wraz z usługą wsparcia technicznego w zakresie instalacji, konfiguracji, zabezpieczenia, odzyskania danych po awarii, itp. w środowisku sprzętowo-programowym administratora (szkoły)**	• Kontrola dostępu do infrastruktury, aplikacji i baz danych. • Dostęp do danych otrzymują wyłącznie osoby wskazane przez przetwarzającego na zlecenie administratora (czynności związane z modyfikacją funckjonalności, konserwacyjne, naprawcze).	**Zespół Szkół Zawodowych XYZ w Krakowie** ul. XYZ 13, sekretariat@ZSZ-XYZ.pl tel. 12 345 678 945	**Nie dotyczy**	**Nie dotyczy**	**Imię Nazwisko** iod@ZSZ-XYZ.edu.pl tel.: 123 456 789	**30 września 2021 r**	**Nie dotyczy**	**Nie dotyczy**	**Nie dotyczy** **(dane przetwarzane są w prywatnej infrastrukturze przetwarzającego)**	**Nie dotyczy**

Źródło: *Rejestrowanie czynności przetwarzania. Poradnik Prezesa UODO*, https://uodo.gov.pl/pl/123/214, [dostęp: 27.11.2020]

w odniesieniu do wszystkich prowadzonych procesów przetwarzania danych osobowych[279]. Brak szczegółowego wskazania układu wymaganych informacji w poszczególnych rejestrach oznacza, że administrator danych lub podmiot przetwarzający może przyjąć dowolny układ informacji dotyczących poszczególnych czynności przetwarzania. Na przykład w odniesieniu do pozycji wskazanej w art. 30 ust. 1 lit. e RODO, w rejestrze czynności przetwarzania dotyczącej informacji o przekazaniu danych osobowych do państwa trzeciego lub organizacji międzynarodowej, administrator może podzielić te informacje na mniejsze jednostki, np. na dwie podpozycje, takie jak: (a) informacja o przekazaniu danych osobowych do państwa trzeciego lub organizacji międzynarodowej ze wskazaniem nazw tych państw/organizacji oraz (b) informacja o zastosowanych zabezpieczeniach w przypadku przekazania na podstawie art. 49 ust. 1 akapit drugi RODO.

Biorąc pod uwagę fakt, że dany administrator prowadzi rejestr wszystkich czynności przetwarzania, które realizowane są w jego organizacji, rejestr czynności powinien być tak skonstruowany, aby dla każdej czynności nie było potrzeby powtarzania informacji o nazwie i danych kontaktowych administratora, a także – gdy ma to zastosowanie – o nazwie i danych kontaktowych przedstawiciela administratora oraz Inspektora Ochrony Danych. Ponadto mając na uwadze fakt, że dany administrator może wykonywać określone czynności jako ich administrator, inne zaś jako współadministrator, celowe jest aby:

1) informacje o nazwie administratora (i jego przedstawiciela), danych kontaktowych, danych kontaktowych IOD umieścić jednorazowo, np. na stronie tytułowej rejestru,
2) dla każdego wpisu w rejestrze czynności na pierwszej pozycji umieścić nazwę lub opis czynności przetwarzania, a następnie informacje o danej czynności wymienione w art. 30 ust. 1 punkty od b) do g) oraz w punkcie 6 rozporządzenia.

W przypadku rejestru kategorii czynności przetwarzania, poszczególne wpisy (rekordy) rejestru powinny być uporządkowane według kategorii przetwarzania, tj. rodzaju usług świadczonych na rzecz administratorów. Biorąc pod uwagę fakt, że każdy rejestr odnosi się do kategorii czynności przetwarzania świadczonych przez jeden podmiot, celowe jest, aby:

1) informacje o nazwie podmiotu przetwarzającego, jego danych kontaktowych, nazwie i danych kontaktowych przedstawiciela, a także nazwisku i danych kontaktowych IOD umieszcza się jednorazowo np. na stronie tytułowej przedmiotowego rejestru,
2) dla każdego wpisu w rejestrze kategorii czynności przetwarzania na pierwszej pozycji umieścić nazwę danej „kategorii czynności przetwarzania" (rodzaj usługi) jako wartość pozwalającą pogrupować wszystkie wpisy, a następnie nazwę i dane kontaktowe administratora danych, dla którego dana usługa jest wykonywana, nazwę i dane kontaktowe, przedstawiciela administratora – jeśli dotyczy oraz, nazwisko

[279] *Wskazówki i wyjaśnienia dotyczące obowiązku rejestrowania czynności i kategorii czynności przetwarzania określonego w art. 30 ust. 1 i 2 RODO*, Urząd ds. Ochrony Danych Osobowych, file:///C:/Users/adwok/Downloads/Wskaz%C3%B3wki%20i%20wyja%C5%9Bnienia%20dotycz%C4%85ce%20obowi%C4%85zku%20z%20art.%2030%20ust.%201%20i%202%20RODO.pdf, [dostęp: 27.11.2020].

i dane kontaktowe wyznaczonego przez niego IOD. Należy zamieścić także informacje wskazane w art. 30 ust. 2 lit. c i d, oraz te, o których mowa w punkcie 8 rozporządzenia.

Co istotne, rozporządzenie ustanawia wymóg prowadzenia rejestrów w formie pisemnej (art. 30 ust.3 RODO), przy czym przepis nie narzuca standardów dotyczących postaci, w jakiej rejestry powinny być prowadzone, wskazując, że może to być postać zarówno papierowa, jak i elektroniczna. Administrator lub podmiot przetwarzający oraz – gdy ma to zastosowanie – ich przedstawiciele udostępniają rejestr na żądanie organu (np. w celu realizacji kontroli).

Obowiązek raportowania naruszenia bezpieczeństwa danych do organu nadzorczego

Przepisy ochrony danych osobowych przewidują szereg wymogów odnoszących się do technicznych i organizacyjnych zabezpieczeń, które mają zapobiegać naruszeniom bezpieczeństwa danych. Należy jednak mieć na uwadze, że nawet najlepsze zabezpieczenia nie są gwarancją skutecznej ochrony. W praktyce jednak zdarzają się przypadki przełamania zabezpieczeń, ich obchodzenia bądź naruszenia ochrony danych w inny sposób. Paweł Fajgielski zauważa, że właśnie „dlatego oprócz regulacji odnoszących się do zabezpieczeń, istotne są prawne mechanizmy, które mają pozwolić na reagowanie w sytuacjach naruszeń i minimalizowanie ich negatywnych następstw. Prawodawca wychodzi z założenia, że informowanie o fakcie naruszenia może pozwolić na reakcję, która daje szansę uniknąć negatywnych skutków tego naruszenia bądź pozwala je znacznie ograniczyć. Dlatego do regulacji prawnych wprowadzane są mechanizmy przewidujące obowiązek informowania o naruszeniu ochrony danych polegające na nałożeniu na podmiot, w strukturze którego miało miejsce naruszenie, obowiązku poinformowania o fakcie naruszenia odpowiednich organów oraz osób, których dane dotyczą, po to, aby ograniczyć negatywne konsekwencje, jakie może pociągać za sobą naruszenie. Nakładanie takich obowiązków jest istotne także dlatego, że podmioty, w których naruszenie nastąpiło, nie są zainteresowane ujawnianiem tego rodzaju informacji, zazwyczaj starają się te informacje ukryć, aby nie narazić na szwank swojej reputacji i nie utracić zaufania klientów. Konieczność ujawnienia informacji o naruszeniu ochrony danych wiąże się z podjęciem działań naprawczych, a także zapobiegających wystąpieniu naruszeń w przyszłości. Informowanie o naruszeniu nabiera szczególnego znaczenia w związku ze stale wzrastającą skalą procederu kradzieży tożsamości”[280].

[280] Pierwsze konstrukcje prawne przewidujące obowiązek informowania o naruszeniu ochrony danych wprowadzone zostały w USA, przy czym amerykańska koncepcja obowiązku zawiadamiania o naruszeniach koncentruje się przede wszystkim na informowaniu osób, których naruszenie dotyczy, a niejako uzupełniająco – w szczegółowo określonych przypadkach – przepisy nakazują zawiadamiać odpowiednie organy. Nieco inną koncepcję obowiązku informowania o naruszeniach przyjęto w prawie unijnym. Wprowadzony w 2009 r. do przepisów dyrektywy 2002/58/WE dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej, wskutek jej nowelizacji, obowiązek zawiadamiania o naruszeniu ochrony danych dotyczy zawiadamiania organu nadzorczego, natomiast osoby, których dane dotyczą, mają być zawiadomione w przypadku, gdy naruszenie może wywrzeć niekorzystny wpływ na ich dane osobowe lub prywatność. W dyrektywie 2002/58 zdefiniowano pojęcie naruszenia danych osobowych; określono zasady powiadamiania; minimalne wymogi, jakie powinno zawierać powiadomienie, a także przewidziano obowiązek prowadzenia rejestru naruszeń ochrony danych osobowych. Przewidziany przepisami wskazanej powyżej dyrektywy obowiązek jest jednak ograniczony jedynie do podmiotów świadczących usługi w sektorze łączności elektronicznej. Zob. *Amerykański system ochrony praw człowieka*, red. J. Jaskiernia, Toruń 2015. Zob. też P. Fajgielski, *Informowanie o naruszeniu ochrony danych osobowych w świetle przepisów ogólnego rozporządzenia o ochronie danych* [w:] *Ogólne rozporządzenie o ochronie danych. Aktualne problemy prawnej ochrony danych osobowych*, red. Sibiga G., Warszawa 2016. Por. Oświadczenie 01/2019 w sprawie amerykańskiej ustawy

Przez naruszenie ochrony danych osobowych – zgodnie z art. 4 pkt 12 rozporządzenia – rozumieć należy „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". Naruszenie bezpieczeństwa, które kwalifikowane jest jako naruszenie ochrony danych, może być przypadkowe (niezamierzone), bądź bezprawne (tj. naruszające przepisy), może polegać na działaniu bądź zaniechaniu, którego skutkiem jest zniszczenie bądź utrata danych (np. usunięcie), ich modyfikacja (np. zmiana treści danych), ujawnienie osobie, która nie jest uprawniona lub uzyskanie dostępu do danych przez osobę nieuprawnioną. Naruszenia mogą odnosić się do różnych czynności przetwarzania danych, w szczególności ich przechowywania bądź przesyłania.

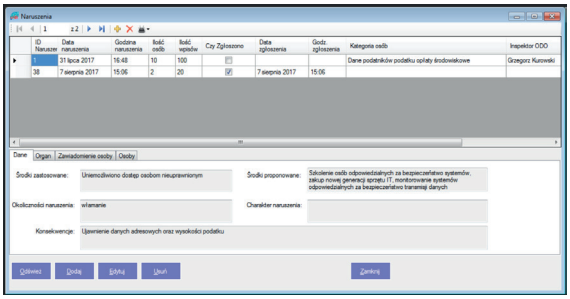
Artykuł 33 rozporządzenia w swojej treści w całości poświęcony jest kwestii naruszeń. Zgodnie z przepisem w przypadku przełamania systemu ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu tegoż naruszenia – powinien zgłosić je organowi nadzorczemu, 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. Zgłoszenie musi 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. Jeżeli – i w zakresie w jakim – informacji nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki. Należy pamiętać, iż sposób w jaki organ dowiedział się o naruszeniu (w szczególności, czy i w jakim stopniu administrator lub procesor zgłosili naruszenie) jest brane pod uwagę przy ustalaniu ewentualnej kary finansowej[281].

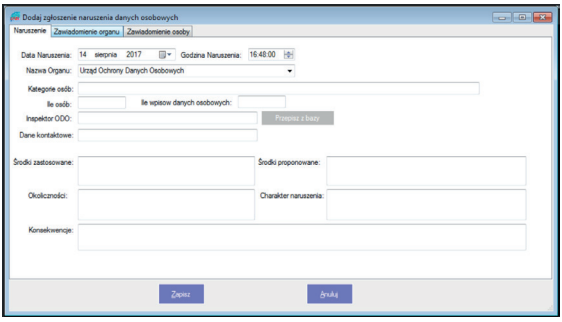
Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym ich okoliczności, skutki oraz podjęte działania zaradcze – nawet jeżeli nie zdecydował się na powiadomienie organu nadzorczego (co wynika wprost ust. 4 omawianego przepisu).

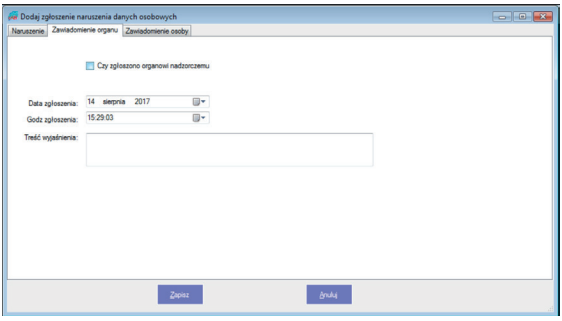
o wypełnianiu obowiązków podatkowych w stosunku do rachunków posiadanych za granicą (Foreign Account Tax Compliance Act; FATCA), przyjęte 25 lutego 2019 r., Europejska Rada Ochrony Danych.

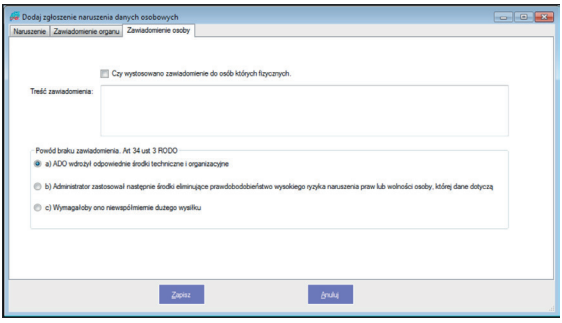
[281] Szerzej zob. Wytyczne 1/2021 w sprawie przykładów dotyczących zgłaszania naruszeń ochrony danych, przyjęte 14 stycznia 2021r., Europejska Rada Ochrony Danych.

RYSUNEK 13 System ewidencjonowania i zgłaszania naruszeń (oprogramowanie eABI)









Źródło: *Rejestr naruszeń ochrony danych osobowych*, eABI, http://www.eabi.pl/blog/rejestr-narusze%C5%84-ochrony-danych-osobowych, [dostęp: 17.12.2021]

Obowiązek raportowania incydentów w ramach systemu ochrony danych osobowych nie jest ani pierwszym, ani jedynym tego typu instrumentem prawnym. Podobne istnieją w ramach systemu cyberbezpieczeństwa[282], usług telekomunikacyjnych[283], czy bankowości[284].

Dokumentacja naruszeń musi pozwolić organowi nadzorczemu na zweryfikowanie stanu faktycznego wraz z tego tytułu konsekwencjami prawnymi. Oznacza to, że w sytuacji, w której administrator nie ma obowiązku poinformowania organu nadzorczego o naruszeniu, musi i tak odnotować je w swojej dokumentacji. „Dokumentacja ta powinna pozwolić organowi nadzorczemu na weryfikowanie przestrzegania wymogów określonych w art. 33 rozporządzenia. Również ten przepis nasuwa wątpliwości interpretacyjne. Jedna z nich dotyczy tego, czy obowiązek dokumentacyjny pokrywa się z obowiązkiem zawiadamiania organu o naruszeniu ochrony danych, czy też jego zakres przedmiotowy jest szerszy. Literalna wykładnia prowadzi do odpowiedzi, że zakres obowiązku dokumentacyjnego jest szerszy, gdyż użycie w przepisie sformułowania „wszelkie naruszenia" sugeruje, że chodzi nie tylko o naruszenia, które mają być przedmiotem zgłoszeń kierowanych do organu nadzorczego, ale także o inne naruszenia (również te, gdy jest mało prawdopodobne, aby naruszenie ochrony danych skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych). Jednak taka wykładnia budzi poważne wątpliwości z punktu widzenia zasadności wprowadzania tego rodzaju obowiązku, a ze względów praktycznych jej przyjęcie oznaczałoby poważne utrudnienie działalności administratorów"[285]. W sytuacji, w której naruszenie ochrony danych osobowych niesie wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator powinien również bez zbędnej zwłoki zawiadomić osobę, której dane dotyczą o takim naruszeniu – jasnym i prostym językiem. Taki wymóg wprowadza przepis art. 34 rozporządzenia[286].

[282] . W przestrzeni telekomunikacyjnej istnieje podobny obowiązek nałożony na operatorów usług kluczowych w sektorze telekomunikacyjnym w ramach sektorowego zespołu cyberbezpieczeństwa. Tzw. „incydent poważny" należy tam zgłosić niezwłocznie, nie później niż w ciągu 24 godzin od momentu jego wykrycia, przy czym za „incydent poważny" należy rozumieć incydent, który powoduje lub może powodować poważnie obniżenie jakości lub przerwanie ciągłości świadczenia usługi kluczowej. Kryteria klasyfikacji incydentu poważnego znajdują się w rozporządzeniu Rady Ministrów z dnia 31 października 2018 r. w sprawie progów uznania incydentu za poważny (Dz.U. 2018 poz. 2180). Zob. ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2018 poz. 1560). Por. Oświadczenie 2/2021 w sprawie nowych postanowień Konwencji Rady Europy o cyberprzestępczości (Konwencja Budapeszteńska), przyjęte 2 lutego 2021 r., Europejska Rada Ochrony Danych.

[283] W dniu 27 września 2018 r. weszły w życie rozporządzenia określające kryteria, po spełnieniu których naruszenie należy uznać za naruszenie o istotnym wpływie na funkcjonowanie sieci lub usług. W takim przypadku przedsiębiorca telekomunikacyjny ma obowiązek niezwłocznego przekazania informacji o naruszeniu Prezesowi UKE na wzorze formularza, który został określony w drugim rozporządzeniu (nowy wzór formularza). Powstanie obowiązku uzależnione jest od czasu braku dostępności lub ograniczenia usługi oraz liczby użytkowników tej usługi dotkniętych naruszeniem. Zgłoszeniu podlegają również naruszenia skutkujące pozbawieniem możliwości wykonywania połączeń z numerami alarmowymi przez co najmniej 10 000 użytkowników. Informowanie Prezesa UKE o naruszeniu bezpieczeństwa i integralności sieci lub usług telekomunikacyjnych należy realizować poprzez formularz elektroniczny „Informowanie o naruszeniu bezpieczeństwa lub integralności sieci lub usług telekomunikacyjnych, które miało istotny wpływ na funkcjonowanie sieci lub usług. Zob. (1) rozporządzenie Ministra Cyfryzacji z dnia 20 września 2018 r. w sprawie kryteriów uznania naruszenia bezpieczeństwa lub integralności sieci lub usług telekomunikacyjnych za naruszenie o istotnym wpływie na funkcjonowanie sieci lub usług (Dz. U. z 2018r., poz. 1830); (2) rozporządzenie Ministra Cyfryzacji z dnia 20 września 2018 r. w sprawie wzoru formularza do przekazywania informacji o naruszeniu bezpieczeństwa lub integralności sieci lub usług telekomunikacyjnych, które miało istotny wpływ na funkcjonowanie sieci lub usług (Dz. U. z 2018r., poz. 1831).

[284] W dniu 20 czerwca 2018 r. weszły w życie przepisy wprowadzające obowiązek raportowania do organu nadzoru przez dostawców usług płatniczych informacji o poważnych incydentach operacyjnych lub poważnych incydentach związanych z bezpieczeństwem, w tym w charakterze informacyjnym. Zgodnie z art. 32g ustawy dostawca przekazuje niezwłocznie KNF lub innemu właściwemu organowi nadzoru informację o poważnym incydencie operacyjnym lub incydencie związanym z bezpieczeństwem, w tym o charakterze teleinformatycznym. Jeżeli incydent ma lub może mieć wpływ na interesy finansowe użytkowników, dostawca bez zbędnej zwłoki powiadamia o incydencie użytkowników korzystających z usług tego dostawcy oraz informuje ich o dostępnych środkach, które mogą podjąć w celu ograniczenia negatywnych skutków incydentu. Zob. ustawa z 10 maja 2018 r. o zmianie ustawy o usługach płatniczych oraz niektórych innych ustaw (Dz. U. z 2018 r., poz. 1075).

[285] Zob. P. Fajgielski, *Informowanie o naruszeniu ochrony danych osobowych w świetle przepisów ogólnego rozporządzenia o ochronie danych*, Monitor Prawniczy 2016, nr 20.

[286] Przepis wprowadza też wyjątki o obowiązku zawiadomienia. Zawiadomienie nie jest wymagane, w następujących przypadkach: (a) administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych; (b) administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą; (c) wymagałoby ono niewspółmiernie dużego wysiłku. Jeżeli administrator nie zawiadomił jeszcze osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, organ nadzorczy – biorąc pod uwagę prawdopodobieństwo, że to naruszenie ochrony danych osobowych spowoduje wysokie ryzyko – może od niego tego zażądać organ nadzorczy. Zob. art. 34

Należy wyeksponować, iż prawodawca europejski nałożył obowiązek zawiadamiania o naruszeniu także na podmiot przetwarzający, a więc – zgodnie z przepisem art. 4 pkt 8 rozporządzenia – na osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora (procesora). Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych ma obowiązek bez zbędnej zwłoki zgłosić ten fakt administratorowi[287]. Rozporządzenie wprowadziło także szereg innych regulacji względem procesora. Po pierwsze zakaz powierzania dalej przetwarzania danych osobowych bez zgody administratora. Po drugie nakaz prowadzenia rejestru wszystkich kategorii czynności przetwarzania danych osobowych dokonywanych w imieniu administratora. Po trzecie nakaz powołania Inspektora Ochrony Danych, jeśli chce realizować zlecenia wymagające przetwarzania niektórych kategorii przetwarzania (np. przetwarzanie danych wrażliwych na dużą skalę). Nadto procesor ma również obowiązek udostępnić przedmiotowy rejestr na żądanie organu nadzorczego oraz obowiązek.

W tym zakresie za konieczny należy uznać obowiązek dokładnego sprecyzowania pozycji stron powierzenia: administratora i procesora. Jest to o tyle istotne, iż jeżeli podmiot przetwarzający, wbrew ustaleniom określi cele i sposoby przetwarzania danych, uznaje się go za administratora w odniesieniu do tego przetwarzania. Zatem jeśli dane powierzy się procesorowi w celu wyznaczonym przez administratora, a on postanowi zmienić pierwotny cel i wykorzystać te dane osobowe w celu oferowania innych produktów i usług stanie się on automatycznie administratorem tych danych.

Wprowadzenie obowiązku raportowania do urzędu nadzoru o incydentach należy – z perspektywy przedsiębiorców – uznać za kolejny, dodatkowy obowiązek prawny wymagający przygotowania organizacji do sprawnego reagowania. Wymusza to na administratorach konieczność wdrożenia większych niż dotychczas mechanizmów zabezpieczenia danych osobowych, a tym samym zaangażowania środków (ich uwzględnienia w budżetach). Trzeba wreszcie pamiętać, że informowanie o naruszeniu bezpieczeństwa, szczególnie istotnych klientów, może być bardzo kosztowne, nie tyle operacyjnie, co wizerunkowo.

Poszerzenie katalogu danych wrażliwych (sensytywnych)

Zgodnie z art. 4 rozporządzenia dane osobowe oznaczają 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,

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 (Dz. Urz. UE L 119 z dn. 4.05.2016, s. 1–88).

[287] Tak ogólnie sformułowanie obowiązku procesora prowadzi do szeregu wątpliwości. Przykładowo czy podmiot przetwarzający powinien informować administratora o każdym naruszeniu ochrony danych, czy też nie musi tego robić w przypadku, gdy jest mało prawdopodobne, aby naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych? Wykładnia literalna prowadzi do wniosku, że podmiot przetwarzający powinien zgłaszać administratorowi o każdym przypadku naruszenia ochrony danych (ponieważ w przepisie nie zostało zawarte ograniczenie tego obowiązku), natomiast wykładnia funkcjonalna skłaniać może do przyjęcia wniosku, że tylko w przypadku naruszeń ochrony danych, które mogą skutkować ryzykiem naruszenia praw lub wolności osób fizycznych, zawiadamianie administratora powinno być dokonywane. Po drugie, czy w przypadku uzyskania przez administratora danych zgłoszenia od podmiotu przetwarzającego, na administratorze ciąży obowiązek zgłoszenia tego faktu organowi nadzorczemu? Zob. P. Fajgielski, *Informowanie o naruszeniu ochrony danych osobowych w świetle przepisów ogólnego rozporządzenia o ochronie danych*, Monitor Prawniczy 2016, nr 20.

numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy IP, adres zamieszkania lub zameldowania, czy numeru telefonu. Rozporządzenie nie wymienia ich wprost, jednak ze względu na fakt, że właśnie te informacje najdokładniej określają konkretną osobę i są podawane najczęściej, funkcjonują w doktrynie jako dane osobowe „zwykłe". Za takim ich zaklasyfikowaniem przemawia fakt, że ich zdobycie nie wymaga nadzwyczajnych nakładów czasu, środków ani kosztów.

RYSUNEK 14 Kategorie danych osobowych - RODO

Dane zwykłe Art. 6 RODO	Szczególne kategorie danych osobowych (dane wrażliwe) Art. 9 RODO	Tzw. dane wrażliwe Art. 10 RODO
- imię, - nazwisko, - adres zamieszkania, - PESEL, - NIP, - numer i seria dowodu osobistego, - wykształcenie, - zawód, - płeć, - numer telefonu.	- pochodzenie rasowe lub etniczne, - poglądy polityczne, - przekonania religijne lub światopoglądowe, - przynależność do związków zawodowych, - dane genetyczne, - dane biometryczne, - dane dotyczące zdrowia, - dane dotyczące seksualności lub orientacji seksualnej.	- dane dotyczące wyroków skazujących i naruszeń prawa.

Źródło: *Ochrona danych osobowych pracownika, czyli RODO a pracodawca*, https://ipersonel.pl/baza-wiedzy-ochrona-danych-osobowych-pracownika-czyli-rodo-a-pracodawca/, [dostęp: 17.12.2020]

RODO wyróżnia tzw. dane wrażliwe, które w rozporządzeniu zostały określone mianem „danych szczególnych kategorii". Celem wyodrębnienia i objęcia zwiększoną ochroną danych sensytywnych – w stosunku do pozostałych danych (tzw. „zwykłych") – jest zwiększenie poziomu ochrony dla tej części danych, której ujawnienie narażone jest na ryzyko naruszenia podstawowych praw i wolności. Ich przetwarzanie mogłoby w znacznym stopniu naruszyć prywatność, a nawet intymność ich właściciela, narazić go na dyskryminację, infamię lub ośmieszenie. RODO nie definiuje wprost pojęcia wrażliwych (sensytywnych) danych osobowych, jednak w przepisach dotyczących zasad przetwarzania danych, w art. 9 wymieniono informacje podlegające szczególnej ochronie. Tym samym można stwierdzić, iż artykuł 9 ust. 1 rozporządzenia wprowadza zamknięty katalog danych wrażliwych. 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[288].

[288] Akt prawny z 1997 roku ustanawiał następujący katalog danych wrażliwych: pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania

W porównaniu do katalogu danych sensytywnych zestawionego ustawą z 1997 roku, zupełną nowością jest włączenie danych biometrycznych do zbioru danych wrażliwych. Wcześniej to były dane zwykłe, a wszelkie ograniczenia miały charakter indywidualnych decyzji administracyjnej podmiotu nadzorczego. Aby zrozumieć charakter danych biometrycznych należy odwołać się do biometrii, jako dziedziny nauki. Zajmuje się ona pomiarami istot żywych w celu określenia ich indywidualnych cech wyróżniających, pozwalających na jednoznaczne identyfikowanie tych istot. W przypadku ludzi dotyczy to m.in. takich cech jak: (a) owal twarzy, rozkład punktów charakterystycznych (oczy, usta) lub temperatur na twarzy, (b) geometria (kształt) ucha, (c) układ naczyń krwionośnych na dłoni lub przegubie ręki, (d) kształt linii zgięcia wnętrza dłoni. Biometria interesuje się także cechami behawioralnymi, związanymi z zachowaniem, w tym m.in. takimi jak: (a) sposób chodzenia, (b) podpis odręczny, (c) sposób pisania na klawiaturze, (d) cechy charakterystyczne ruchu ust i poruszania gałki ocznej. Biometria wykorzystywana jest głównie w takich dziedzinach jak: weryfikacja tożsamości, autoryzacja dostępu do systemów informatycznych, czy identyfikacja.

Różnica między przesłankami dopuszczalności przetwarzania danych zwykłych i wrażliwych wynika z odwrócenia podstaw przetwarzania. Przetwarzanie danych zwykłych jest zgodne z prawem we wszystkich przypadkach określonych w art. 6 rozporządzenia, a jedną z alternatywnych podstaw jest prawnie uzasadniony interes realizowany przez administratora lub przez stronę trzecią. Uzasadniony interes to otwarty katalog, należy więc przyjąć, że przetwarzanie danych zwykłych nie podlega ogólnemu zakazowi. Natomiast przetwarzanie danych wrażliwych jest generalnie zabronione, a zakaz nie ma zastosowania, jeżeli spełniony jest jeden z warunków określonych w art. 9 ust. 2 rozporządzenia[289], tj.:

a) osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, chyba że prawo Unii lub prawo państwa członkowskiego przewidują, iż osoba, której dane dotyczą, nie może uchylić zakazu;
b) przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy,

religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, dane o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz dane dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym. Zob. art. 27 ust. 1 ustawy dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 1997 nr 133 poz. 883 z późn. zm.).

[289] Przesłanki legalizujące przetwarzanie danych wrażliwych na postawie ustawy z 1997 roku: (1) osoba, której dane dotyczą, wyraziła na to zgodę na piśmie, chyba że chodziło o usunięcie dotyczących jej danych, (2) przepis szczególny innej ustawy zezwalał na przetwarzanie takich danych bez zgody osoby, której dane dotyczą, i stwarzał pełne gwarancje ich ochrony, (3) przetwarzanie takich danych było niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby, gdy osoba, której dane dotyczą, nie była fizycznie lub prawnie zdolna do wyrażenia zgody, do czasu ustanowienia opiekuna prawnego lub kuratora, (4) było to niezbędne do wykonania statutowych zadań kościołów i innych związków wyznaniowych, stowarzyszeń, fundacji lub innych niezarobkowych organizacji lub instytucji o celach politycznych, naukowych, religijnych, filozoficznych lub związkowych, pod warunkiem, że przetwarzanie danych dotyczyło wyłącznie członków tych organizacji lub instytucji albo osób utrzymujących z nimi stałe kontakty w związku z ich działalnością i zapewnione były pełne gwarancje ochrony przetwarzanych danych, (5) przetwarzanie dotyczyło danych, które były niezbędne do dochodzenia praw przed sądem, (6) przetwarzanie było niezbędne do wykonania zadań administratora danych odnoszących się do zatrudnienia pracowników i innych osób, a zakres przetwarzanych danych był określony w ustawie, (7) przetwarzanie było prowadzone w celu ochrony stanu zdrowia, świadczenia usług medycznych lub leczenia pacjentów przez osoby trudniące się zawodowo leczeniem lub świadczeniem innych usług medycznych, zarządzania udzielaniem usług medycznych i były stworzone pełne gwarancje ochrony danych osobowych, (8) przetwarzanie dotyczyło danych, które zostały podane do wiadomości publicznej przez osobę, której dane dotyczą, (9) było to niezbędne do prowadzenia badań naukowych, w tym do przygotowania rozprawy wymaganej do uzyskania dyplomu ukończenia szkoły wyższej lub stopnia naukowego; publikowanie wyników badań naukowych nie mogło następować w sposób umożliwiający identyfikację osób, których dane zostały przetworzone, (10) przetwarzanie danych było prowadzone przez stronę w celu realizacji praw i obowiązków wynikających z orzeczenia wydanego w postępowaniu sądowym lub administracyjnym. Zob. art. 27 ust. 2 ustawy dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 1997 nr 133 poz. 883 z późn. zm.).

zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii lub prawem państwa członkowskiego, lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą;

c) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody;

d) przetwarzania dokonuje się w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych, pod warunkiem że przetwarzanie dotyczy wyłącznie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami oraz że dane osobowe nie są ujawniane poza tym podmiotem bez zgody osób, których dane dotyczą;

e) przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą;

f) przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy;

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;

h) przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego lub zgodnie z umową z pracownikiem służby zdrowia i z zastrzeżeniem warunków i zabezpieczeń;

i) przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub 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;

j) przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89,

ust. 1 rozporządzenia, na podstawie prawa Unii lub prawa państwa członkowskiego, które 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.

W uzupełnieniu należy zasygnalizować, iż dane osobowe dotyczące wyroków skazujących oraz naruszeń prawa należą do szczególnie chronionych, choć nie są danymi wrażliwymi w rozumieniu art. 9 ust. 1 rozporządzenia. Ich przetwarzanie jest dopuszczalne wyłącznie pod nadzorem władz publicznych lub jeżeli wprost jest dozwolone przepisami szczególnymi. Stypizuje to wprost art. 10 rozporządzenia. Przetwarzania danych osobowych dotyczących wyroków skazujących oraz naruszeń prawa lub powiązanych środków bezpieczeństwa, na podstawie art. 6 ust. 1, wolno dokonywać wyłącznie pod nadzorem władz publicznych lub jeżeli przetwarzanie jest dozwolone prawem Unii lub prawem państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw i wolności osób, których dane dotyczą. Wszelkie kompletne rejestry wyroków skazujących są prowadzone wyłącznie pod nadzorem władz publicznych[290].

RODO zezwala na to, by państwa członkowskie mogły zachować lub wprowadzić dalsze warunki, w tym ograniczenia w odniesieniu do przetwarzania danych genetycznych, danych biometrycznych lub danych dotyczących zdrowia.

Modyfikacja konstrukcji zgody na przetwarzanie danych

Zasady przetwarzania danych osobowych określone zostały w art. 5 rozporządzenia. Dane osobowe muszą być:

a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość");
b) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; 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 rozporządzenia za niezgodne z pierwotnymi celami („ograniczenie celu");
c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych");

[290] Przykładowo w Polsce – poza systemami obejmującymi państwa strefy Schengen jak: Schengen Information System i Visa Information System – występują systemy krajowe, w tym m.in. (a) Krajowy System Informacyjny Policji (KSIP), czy (b) Krajowy Rejestr Karny. Zgodnie z art. 21nb ust. 1 ustawy o Policji Komendant Główny Policji prowadzi Krajowy System Informacyjny Policji („KSIP"), będący zestawem zbiorów danych, w którym przetwarza się informacje, w tym dane osobowe, w związku z realizacją zadań ustawowych. Komendant Główny Policji jako administrator danych rozpatruje wnioski osób dotyczące przetwarzania ich danych w Krajowym Systemie Informacyjnym Policji. Z kolei administratorem danych zgromadzonych w Krajowym Rejestrze Karnym jest Minister Sprawiedliwości, który określa szczegółowe zasady i sposób przetwarzania oraz przekazywania danych zawartych w tym Rejestrze. Zob. ustawa z dnia 24 maja 2000 r. o Krajowym Rejestrze Karnym (t.j. Dz.U. z 2021r., poz. 1709). Szerzej na temat ochrony danych osobowych w SIS i VIS zob. A. Rogala-Lewicki, *Dane osobowe w systemach informacyjnych Schengen (SIS, VIS) – ochrona i nadzór instytucjonalny*, Wiedza Prawnicza, Nr 5/2013.

d) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość");
e) 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; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1 rozporządzenia, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą („ograniczenie przechowywania");
f) przetwarzane w sposób zapewniający 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 („integralność i poufność").

Zgodnie z art. 6 rozporządzenia przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z warunków legalizacyjnych, w szczególności:

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[291].

[291] Akapit pierwszy lit. (f) nie ma zastosowania do przetwarzania, którego dokonują organy publiczne w ramach realizacji swoich zadań. Podstawa przetwarzania, o którym mowa w ust. 1 lit. (c) i (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. Podstawa prawna może zawierać przepisy szczegółowe dostosowujące stosowanie przepisów rozporządzenia, w tym: ogólne warunki zgodności z prawem przetwarzania przez

Wyrażenie zgody na przetwarzanie danych osobowych przez osobę, której dane dotyczą było i jest zatem jednym z podstawowych warunków dopuszczalności przetwarzania danych osobowych[292]. Istotnie zmieniły się natomiast zasady pozyskania ważnej zgody.

RODO wymaga po pierwsze by zgoda była udzielona w formie oświadczenia lub wyraźnego działania, po drugie nowa klauzula zgody musi również informować o celu przetwarzania danych. Dwie kluczowe zatem zmiany polegały na:

1) zdezaktualizowaniu możliwości wyrażenia zgody w sposób domyślny (zgodę „zwykłą" zastąpiła zgoda „jednoznaczna"),
2) konieczności pozyskania nowej zgody w sytuacji zmiany celu przetwarzania[293].

W momencie, w którym RODO wchodziło w życie, pojawiły się wątpliwości czy nowe zasady pozyskiwania zgód nie implikowały konieczności pozyskania od nowa wszystkich, uzyskanych przed 25 maja 2018 r (na podstawie wcześniejszych przepisów), zgód, i tym samym czy zgody zachowywały dalej swoją ważność. RODO nie zawierało przepisów przejściowych w stosunku do dyrektywy 95/46/WE. Wątpliwości wynikały m.in. z faktu, że poprzedzające RODO przepisy nie nakładały różnych nowych wymogów prawnych (np. obowiązku informowania o prawie do cofnięcia zgody). Każdy administrator musiał ocenić, czy pozyskane przez niego zgody spełniały kryteria opisane w art. 4 pkt 11 (dobrowolności, konkretności, świadomości i jednoznaczności), art. 6 ust. 1 lit. a, w związku z art. 7 oraz art. 9 ust. 2 lit. a rozporządzenia. Niepewność została usunięta stanowiskiem zawartym w Wytycznych Grupy Roboczej art. 29 dotyczących zgody (WP259), jak i opinią polskiego Generalnego Inspektora Ochrony Danych Osobowych. Zgodnie z nimi stare zgody, co do zasady, utrzymały ważność. Należało jednak zbadać czy były one pozyskane zgodnie z zasadami dobrowolności, konkretności, świadomości i jednoznacznego wyrażenia zgody. Ponadto jeżeli zmienił się cel przetwarzania zebranych danych lub potrzebne było pozyskanie zgody na nowo na podstawie innych kryteriów, konieczne było zadośćuczynienie wszystkim obowiązkom wynikającym z RODO[294]. Ważność zachowała zatem zgoda, która równolegle spełniała wymogi rozporządzenia. „Fakt, iż zgoda spełnia standardy ustawy o ochronie danych osobowych, czyli odpowiada wymogom prawnym aktualnym w momencie ich zbierania, nie będzie miał

administratora; rodzaj danych podlegających przetwarzaniu; osoby, których dane dotyczą; podmioty, którym można ujawnić dane osobowe; cele, w których można je ujawnić; ograniczenia celu; okresy przechowywania; oraz operacje i procedury przetwarzania, w tym środki zapewniające zgodność z prawem i rzetelność przetwarzania, w tym w innych szczególnych sytuacjach związanych z przetwarzaniem, o których mowa w rozdziale IX rozporządzenia. Prawo Unii lub prawo państwa członkowskiego muszą służyć realizacji celu leżącego w interesie publicznym, oraz być proporcjonalne do wyznaczonego, prawnie uzasadnionego celu. 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 stanowiących w demokratycznym społeczeństwie niezbędny i proporcjonalny środek służący zagwarantowaniu celów, o których mowa w art. 23 ust. 1 rozporządzenia, administrator – aby ustalić, czy przetwarzanie w innym celu jest zgodne z celem, w którym dane osobowe zostały pierwotnie zebrane – bierze pod uwagę między innymi: (a) wszelkie związki między celami, w których zebrano dane osobowe, a celami zamierzonego dalszego przetwarzania, (b) kontekst, w którym zebrano dane osobowe, w szczególności relację między osobami, których dane dotyczą, a administratorem, (c) charakter danych osobowych, w szczególności czy przetwarzane są szczególne kategorie danych osobowych zgodnie z art. 9 rozporządzenia lub dane osobowe dotyczące wyroków skazujących i naruszeń prawa zgodnie z art. 10 rozporządzenia, (d) ewentualne konsekwencje zamierzonego dalszego przetwarzania dla osób, których dane dotyczą, (e) istnienie odpowiednich zabezpieczeń, w tym ewentualnie szyfrowania lub pseudonimizacji. Zob. art. 6 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 (Dz. Urz. UE L 119 z dn. 4.05.2016, s. 1–88).

[292] Szerzej na temat zgody zob. Opinia 15/2011 w sprawie definicji zgody, WP 187, Grupa robocza art. 29.

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

[294] *Szykuj się do RODO! Kiedy i jaka zgoda na przetwarzanie danych osobowych*, https://poradnik.ngo.pl/c-szykuj-sie-do-rodo-kiedy-i-jaka-zgoda-na-przetwarzanie-danych-osobowych, [dostęp: 24.11.2020].

charakteru decydującego. Również zasada *lex retro non agit* (niedziałania prawa wstecz) nie będzie miała w tym przypadku zastosowania, bowiem konieczność dostosowania zgód do wymogów w żaden sposób nie wpływa na skuteczność i prawidłowość stosunków prawnych ukształtowanych przed wejściem w życie RODO. Punktem odniesienia dla uznania ważności dotychczas zebranych zgód na przetwarzanie danych będą zatem jedynie przepisy RODO zawierające wymagania wobec tej konkretnej podstawy prawnej przetwarzania danych"[295].

Analiza poprawności wszystkich dotychczasowych zgód powinna zatem w pierwszej kolejności uwzględniać to, czy zebrane dotychczas zgody: (a) były opatrzone wyraźnym wskazaniem administratora i określeniem celu przetwarzania danych, (b) nie były dorozumiane z oświadczeń innej treści, czy milczące (niepodjęcie działań nie może oznaczać zgody) lub polegające na domyślnym zaznaczeniu okienek przez usługodawcę, (c) były uzyskane w warunkach swobodnej możliwości ich cofnięcia[296]. Przedmiotem dyskusji w szczególności było brzmienie art. 7 ust. 3 RODO, które wyraźnie wskazuje na konieczność zapewnienia, że zgoda może zostać wycofana w dowolnym momencie. Jej wycofanie musi być równie łatwe, jak jej wyrażenie, co oznacza, że jeśli zgoda była pozyskana przy użyciu interfejsu użytkownika (na przykład za pośrednictwem strony internetowej, aplikacji, strony logowania, interfejsu urządzenia IoT lub poczty elektronicznej), jej odwołanie powinno być możliwe za pomocą tego samego interfejsu elektronicznego. Owa łatwość odwołania zgody w każdym momencie była decydująca w uznaniu, czy dotychczas zebrane zgody zachowają ważność. Jak podkreślono w Wytycznych Grupy Roboczej art. 29, przepis art. 13 ust. 2 RODO należy rozumieć w sposób, który nie wyklucza ważności zebranych zgód w sytuacji kiedy nie wszystkie informacje określone w tym przepisie zostały przekazane osobie, której dane dotyczą w momencie pozyskiwania zgody (zostały np. zawarte w polityce prywatności). „Jako że nie wszystkie elementy wymienione w artykułach 13 i 14 muszą zawsze występować jako warunek świadomej zgody, rozszerzone obowiązki informacyjne na mocy RODO niekoniecznie przeciwstawiają się ciągłości zgody wyrażonej przed wejściem w życie RODO"[297]. Tożsame stanowisko zajął Generalny Inspektor Ochrony Danych Osobowych.

Mając powyższe na uwadze, administratorzy przetwarzający dane osobowe w Polsce na podstawie zgody wyrażonej na mocy ustawy o ochronie danych osobowych z 1997 roku, co do zasady nie musieli automatycznie pozyskiwać wszystkich zgód na nowo.

Rozporządzenie w ramach nowej definicji legalnej zgody zezwala na to, by zgoda mogła być złożona w innej formie niż pisemna. Dopuszczalna jest zatem forma elektroniczna (np. poprzez e-mail, SMS, portale społecznościowe czy komunikatory). Dopuszczalna jest również forma dokumentowa w rozumieniu art. 773 Kodeksu cywilnego. W pewnych wypadkach możliwa

[295] Stanowisko GIODO w sprawie zachowania ważności zgód na przetwarzanie danych, odnoszące się do dyskusji publicznej na ten temat, opiera się na Wytycznych Grupy Roboczej Art. 29 dotyczących zgody na mocy rozporządzenia 2016/679 (WP259), https://archiwum.giodo.gov.pl/pl/1520281/10303, [dostęp: 24.11.2020].

[296] Szerzej zob. 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.

[297] Wytyczne dotyczące zgody na mocy rozporządzenia 2016/679, przyjęte 28 listopada 2017 r. (17/PL WP259), http://giodo.gov.pl/pl/1520281/10292, [dostęp: 24.11.2020].

jest zgoda w formie ustnej, ale będzie ona miała charakter wyjątkowy. W konsekwencji dla jej ważności potrzebny będzie dobrze udokumentowany materiał dowodowy. Artykuł 4 punkt 11 RODO stanowi, że zgoda musi łącznie spełniać cztery warunki, i być:

- dobrowolna,
- konkretna,
- świadoma,
- oraz jednoznaczne wyrażać wolę.

Z pomocą w wyjaśnieniu tych przesłanek przychodzi preambuła RODO i wytyczne Grupy Roboczej art. 29

Zgodnie z definicją zgoda osoby, której dane dotyczą, oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, w którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego przyzwala na przetwarzanie dotyczących jej danych osobowych. W piśmiennictwie podkreśla się, że przepisy akcentują rolę dobrowolności zgody. Anna Dmochowska zauważa, że „zgoda nie będzie mogła zostać uznana za dobrowolną, jeśli nie można jej wyrazić z osobna na różne operacje przetwarzania danych osobowych bądź w sytuacji gdy od wyrażenia zgody uzależnione będzie wykonanie umowy, jeżeli wyrażenie zgody nie jest niezbędne do jej wykonania”[298]. W ujęciu ogólnym, zgoda jest to każde oświadczenie lub zachowanie, które w danej sytuacji jasno wskazuje, że osoba, której dane dotyczą, dokonała akceptacji proponowanego przetwarzania jej danych osobowych.

Dobrowolność zgody jest zatem oceniana w kontekście sytuacyjnym. Zgoda wyrażona dobrowolnie oznacza, że osoba, która jej udziela, ma wolny wybór, nie jest przymuszona, oraz ma prawo do odmowy lub wycofania zgody w każdej chwili, kiedy tak uważa. Jeżeli odmowa udzielania zgody wywoła negatywne konsekwencje dla odmawiającej osoby, to nie będzie to zgoda dobrowolna[299]. Warto również pamiętać, że dobrowolność zgody jest związana z jej formą. W preambule do RODO wymienia się przykładowe formy wyrażania zgody, takie jak: forma pisemna, także w postaci elektronicznej oraz forma ustnego oświadczenia zainteresowanego. Uzasadnione zatem jest przyjęcie, iż przykładowo wyrażenie przedmiotowej zgody może zostać wyartykułowane poprzez zaznaczenie okienka wyboru podczas przeglądania strony internetowej, czy też zaakceptowanie ustawień technicznych do korzystania z usług portalu informacyjnego. Nie mniej w obrocie prawnym problematycznym pozostaje ujęcie momentu wyraźnego działania i ustalenie jego formy. Co za tym

[298] *Artykul 7 – Warunki wyrażenia zgody*, https://gdpr.pl/baza-wiedzy/akty-prawne/interaktywny-tekst-gdpr/artykul-7-warunki-wyrazenia-zgody, [dostęp: 15.11.2020].

[299] W praktyce powstaje wątpliwość czy jeżeli zgoda jest bezpośrednio związana z daną usługą to odmowa jej wyrażenia jest negatywną konsekwencją. Przykładem może być zapisanie się na szkolenie, które wymaga podania danych do wystawienia faktury. W takiej sytuacji trzeba zwrócić uwagę na dwa aspekty. Po pierwsze czy istnieje inna przesłanka niż zgoda, na podstawie której dane osobowe mogą być przetwarzane. Trzeba przeanalizować artykuł 6 RODO. W tym przykładzie (zapisanie się na szkolenie) będzie to przesłanka zawarta w art. 6 ust. 1 lit. b: przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą. W takim wypadku nie jest konieczne pozyskiwanie zgody. Co więcej nie powinno się tego robić, na co wprost wskazują wytyczne Grupy Roboczej art. 29. Po drugie należy zbadać czy ilość pozyskiwanych danych jest minimalna dla realizacji celu. W przypadku szkolenia może być to imię, nazwisko i e-mail lub inny środek kontaktu (raczej nie ma potrzeby pozyskiwania innych danych, np. adresu zamieszkania). Szerzej 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. Zob. też. K. Szymielewicz, A. Walkowiak, *Autonomia informacyjna w kontekście usług internetowych: o znaczeniu zgody na przetwarzanie danych i ryzykach związanych z profilowaniem*, Monitor Prawniczy 2014, nr 9, s. 29–33.

idzie, za zgodę na przetwarzanie danych nie będzie można uznać milczenia (w przypadku strony internetowej np. okienka domyślnie zaznaczonego przez administratora tej strony).

Motyw 43 RODO zwraca szczególną uwagę w tym kontekście na sytuację, w której istnieje wyraźny brak równowagi pomiędzy administratorem a osobą, której dane dotyczą, np. w relacji pracodawca – pracownik. Uważa się, że zgoda nie została wyrażona dobrowolnie, gdy na przykład wymaga się wyrażenia zgody na przetwarzanie niepotrzebnych danych osobowych, jako warunku koniecznego do wykonania umowy lub usługi (kiedy przykładowo umożliwienie skorzystania z oferty zależy od udzielenia zgody na przetwarzanie danych dla celów marketingowych)[300].

Konkretność zgody z kolei odnosi się do jej precyzyjnego sformułowania. Zgoda powinna wprost wskazywać przesłanki, cel i zakres, w jakich dane będą przetwarzane. Za konkretną, czy precyzyjną nie jest uważana zgoda, która jest widocznie niewyodrębnioną częścią umowy, a także zgoda będąca częścią regulaminów świadczenia usług. Możliwość wyrażenia zgody na przetwarzanie danych osobowych powinna być jasno rozdzielona od treści normatywnej umów lub innych aktów. Niedopuszczalne jest zatem zbieranie zgód blankietowych, zbiorczych, czy ogólnych.

Należy również wyraźnie oddzielić informacje związane z uzyskaniem zgody od informacji dotyczących innych kwestii. W okolicznościach, w których zgoda na przetwarzanie danych osobowych jest jedynie częścią innego dokumentu, samo oświadczenie o wyrażeniu zgody na przetwarzanie danych osobowych musi zostać jednoznacznie wyodrębnione. Podobnie w przypadku pozyskiwania zgody na różne cele przetwarzania. Powinny one zostać w sposób wyraźny od siebie odseparowany. W trakcie tworzenia formularza zgody, czy zgód administrator danych ma zatem obowiązek dostosowania się do wszystkich zasad, i uwzględnienia zasad pozyskiwania zgód w procesie przetwarzania danych. Podmiot, który udziela zgody na przetwarzanie danych osobowych ma prawo do podstawowych informacji, chociażby na czyją rzecz udziela zgody, w jakim celem, oraz które dane będą przedmiotem przetwarzania.

Ważna zgoda wymaga jednoznacznego okazania w formie oświadczenia lub wyraźnego działania potwierdzającego, co oznacza, że osoba, której dane dotyczą, musi podjąć celowe działanie w celu wyrażenia zgody na określone przetwarzanie. Niedopuszczalne jest zatem przyjęcie, że milczenie lub brak działania oznacza zgodę (np. na domyślnie uzupełnionych formularzach internetowych). Administrator musi być w stanie dowodowo wykazać – zgodnie z zasadą rozliczalności – uzyskanie zgody. Ponadto, aby umożliwić podejmowanie świadomych decyzji przez osoby, których dane dotyczą, administratorzy powinni upewnić się, że używają jasnego i dostępnego języka. Zgodnie z Wytycznymi Grupy art. 29 aby zgoda była świadoma, osoba która jej udziela, musi otrzymać co najmniej następujące informacje:

- tożsamość organizacji przetwarzającej dane,

[300] *Kiedy zgoda jest uznana za ważną?*, Komisja Europejska, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/when-consent-valid_pl, [dostęp: 24.11.2020].

- cele, w jakich dane są przetwarzane,
- rodzaj przetwarzanych danych,
- swoje prawo do wycofania wcześniej udzielonej zgody,
- w stosownych przypadkach informację o tym, że dane zostaną wykorzystane do podejmowania decyzji opartych wyłącznie na zautomatyzowanym przetwarzaniu danych, w tym profilowaniu,
- w przypadku, gdy zgoda dotyczy międzynarodowego przekazywania danych, informację o ryzyku przekazania do krajów trzecich, które nie zostały objęte decyzją.

Skutecznej zgody będzie mogła udzielić osoba z pełną zdolnością do czynności prawnych. Wyjątkiem są sytuacje dotyczące usług społeczeństwa informacyjnego (chodzi o umowy i inne usługi, które są zawierane lub przekazywane online). Dotyczy to np. gier online, świadczenia usług w chmurze, czy sprzedaży przez Internet[301]. Rozporządzenie zawiera odniesienia do zgody na przetwarzanie danych dzieci w kontekście korzystania przez nie z usług społeczeństwa informacyjnego. W przypadku dzieci, które nie mają ukończonego 16 roku życia, zgodę w zakresie korzystania przez nie z usług społeczeństwa informacyjnego powinna wyrazić lub zaaprobować osoba sprawująca władzę rodzicielską lub opiekę. Co więcej, administrator danych, przy uwzględnieniu dostępnej technologii, musi podjąć starania, aby możliwa była weryfikacja tego, czy osoba, która sprawuje władzę rodzicielską lub opiekę nad dzieckiem, rzeczywiście wyraziła zgodę lub ją zaaprobowała.

Jest to istotnym *novum* w zakresie wyrażania zgody na przetwarzanie danych osobowych. Przy tym warto zaznaczyć, iż rozporządzenie pozostawia państwom członkowskim prawo, aby przewidziały w prawie krajowym niższą granicę wiekową, która jednak nie może być niższa niż 13 lat. Polskie prawo zezwala na zawieranie niektórych typów umów osobom, które ukończyły 13 rok życia, na przykład umów powszechnie zawieranych w drobnych bieżących sprawach życia codziennego (art. 20 Kodeksu cywilnego). Jednocześnie, jeżeli do wykonania takiej umowy potrzebna jest zgoda na przetwarzanie danych osobowych, to będzie ona nieważna (art. 19 Kodeksu cywilnego) ze względu na opisaną wyżej granicę 16 lat. RODO zatem choć daje cały czas możliwość ustawodawcy krajowemu na zmianę granicy tego wieku, z zastrzeżeniem, iż musi on wynosić minimum 13 lat, to w Polsce nie zdecydowano się, póki co, na podjęcie takich działań[302].

Rozporządzenie w art. 7 ust. 3 wskazuje, że zgoda może być odwołana w każdym momencie, przy czym nie można nakładać negatywnych konsekwencji z tego tytułu. Wycofanie

[301] Zob. (a) Wytyczne 2/2021 w sprawie wirtualnych asystentów głosowych, wersja 2.0, przyjęte 7 lipca 2021r., Europejska Rada Ochrony Danych; (b) Wytyczne 1/2020 w sprawie pojazdów połączonych i aplikacji związanych z mobilnością wersja 2.0, przyjęte 9 marca 2021 r., Europejska Rada Ochrony Danych; (c) 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.

[302] Anna Dmochowska wysuwała przypuszczenia, że w Polsce granica wieku najprawdopodobniej zostanie obniżona do lat 13, co będzie zgodne z wytycznymi KC przyznającemu dziecku w wieku 13 lat ograniczoną zdolność do czynności prawnych. Zob A. Dmochowska A., *Przetwarzanie danych na podstawie zgody* [w:] *Unijna reforma ochrony danych osobowych. Analiza zmian*, red. A. Dmochowska A., Zadrożny M., Warszawa 2016.

zgody musi być równie łatwe jak jej wyrażenie. Odwołanie wywołuje skutek natychmiastowy, czyli od momentu otrzymania oświadczenia woli w tym zakresie. Odwołanie nie wywołuje skutków wstecz. To znaczy, że operacje przetwarzania danych, które były dokonane w czasie gdy zgoda obowiązywała, są zgodne z prawem.

Wreszcie, na każdym administratorze – zgodnie z zasadą przejrzystości – ciąży obowiązek poinformowania osoby, której dane dotyczą, o możliwości odwołania zgody, zanim ta zgoda zostanie wyrażona. Unijny ustawodawca zdecydował się wyróżnić ten konkretny obowiązek informacyjny administratora sytuując go w przepisie określającym warunki wyrażenia zgody. Ten szerszy kontekst można wiązać z koniecznością stworzenia mechanizmów zapewniających możliwość łatwego wycofania zgody, jako jeden z aspektów autonomii informacyjnej osób, których dane dotyczą. Informacje, jak wycofać zgodę, mają w tym kontekście zasadnicze znaczenie.

Pseudonimizacja danych osobowych

Istotną zmianą wynikającą z nowych przepisów w zakresie ochrony danych osobowych, jest kwestia wprowadzenia wymogu pseudonimizacji przetwarzanych danych. Zgodnie z założeniami RODO pseudonimizacja danych osobowych powinna ograniczyć ryzyko naruszeń danych osób, których dane dotyczą, oraz pomóc administratorom wywiązać się z obowiązku ochrony danych. W myśl art. 4 pkt 5 rozporządzenia pseudonimizacja jest definiowana 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. W wyniku pseudonimizacji część danych, dotyczących danej osoby zostaje zastąpiona pseudonimem, dzięki czemu są one chronione.

Pseudonimizacja została wymieniona także w art. 32 rozporządzenia jako jeden ze środków technicznych i organizacyjnych, służących do zapewnienia odpowiedniego stopnia bezpieczeństwa odpowiadającego stopniowi ryzyka naruszenia praw lub wolności osób fizycznych. Z tego też przepisu wynika fakt, że pseudonimizację należy stosować uwzględniając 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. Pseudonimizacja stanowi szczególnie przydatny środek ochrony zwłaszcza w przypadku przetwarzania dużej ilości danych. Stosuje się ją zatem w celu podwyższenia poziomu bezpieczeństwa danych osobowych oraz w celu ochrony danych istotnych dla danej osoby czy przedsiębiorstwa. Administratorzy danych stosują różne metody pseudonimizacji danych, jednak najczęściej używane to:

- tokenizacja – polegająca na zmianie danych na losowo wygenerowany ciąg liczbowy,
- skracanie – polegające na skróceniu danych pozwalających na identyfikację danej osoby fizycznej,

- szyfrowanie tajnym kluczem – polegające na szyfrowaniu danych za pomocą klucza szyfrującego, który w przyszłości może być użyty do odszyfrowania danych.

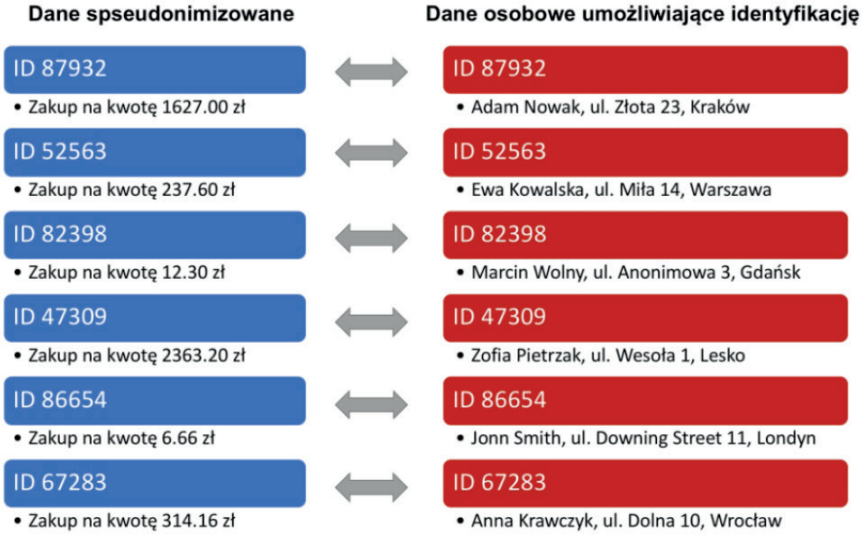
Pseudonimizacja w głównej mierze polega zatem na zamaskowaniu – zastąpieniu informacjami nieczytelnymi dla odbiorcy poufnych informacji. Tytułem przykładu: zastąpienie imienia i nazwiska inicjałami, a w przypadku adresu zamieszkania pierwszymi literami ulicy i miejscowości. Innym przykładem pseudonimizacji danych jest stosowana od pewnego czasu w szkołach publikacja ocen wraz z identyfikatorem ucznia zamiast jego imienia i nazwiska. W trakcie pseudonimizacji należy jednak zachować należyte środki ostrożności, gdyż dane podlegające pseudonimizacji niekiedy mogą w sposób pośredni prowadzić do ustalenia tożsamości osoby, jeżeli zawierają pewne informacje, które w konkretnej grupie, czy społeczności charakteryzują i identyfikują daną osobę. Przykładem takiej pseudonimizacji może być pseudonimizacja wyroków sądowych, gdy postępowanie toczy się przed lokalnym sądem, informacje na jego temat są publiczne znane lokalnej społeczności. W takiej sytuacji, mimo maskowania danych osobowych, podmioty uwikłane w sprawę stają się rozpoznawalne[303]. Jak objaśnia Grzegorz Bernatek „najczęściej stosowanymi technikami pseudonimizacji są:

- szyfrowanie za pomocą tajnego klucza – dane osobowe są nadal przechowywane w zbiorze danych, ale w formie zaszyfrowanej (posiadanie klucza szyfrującego pozwala na pełen dostęp do danych osobowych, a używając szyfrowania, które zachowuje aktualne standardy bezpieczeństwa, możliwość odszyfrowania danych jest możliwa, ale tylko z użyciem klucza szyfrującego),
- funkcje skrótu – polegające na skróceniu dowolnego ciągu znaków o stałej, określonej długości [(dowolnej informacji przydzielany jest unikalny identyfikator, przy czym funkcji tej nie można odwrócić, tak jak w przypadku szyfrowania, jakkolwiek, znając zakres wartości, jakie zostały poddane skracaniu oraz w jaki sposób zostało ono wykonane, możliwe jest odtworzenie funkcji skrótu i uzyskanie prawidłowego zapisu poprzez tzw. atak siłowy (wypróbowanie wszystkich możliwych kombinacji w celu utworzenia tabel korelacji), a funkcje skrótu można podzielić ze względu na wielkości bloku wyjściowego (ilość bitów),
- do niedawna stosowane były funkcje skrótu MD5 oraz SHA-1, zostały on jednak wycofane ze względu na niewystarczający poziom bezpieczeństwa;
- tokenizacja – polega na wykorzystaniu jednokierunkowych mechanizmów szyfrujących opartych na przypisaniu identyfikatora (indeksu, sekwencji lub losowo wygenerowanej liczby) w żaden sposób niezwiązanej z pierwotnymi danymi, przy czym technika ta jest często spotykana w sektorze finansowym do autoryzacji operacji bankowych)"[304].

[303] Szerzej zob. *Reforma ochrony danych osobowych a jawność dostępu do informacji sądowej – aspekty proceduralne*, red. M. Jabłoński, K. Flaga-Gieruszyńska, K. Wygoda, Wrocław 2017. Zob. też M. Mucha, *Ograniczenia zasady jawności i dostępu do informacji – regulacje administracyjnoprawne*, Samorząd Terytorialny 2000, nr 1/2.

[304] Obecne zalecenia amerykańskiej agencji NIST dotyczące stosowania poszczególnych funkcji skrótu mówią, że do nowych aplikacji zalecane są funkcje skrótu z rodziny SHA-2, a w przyszłości funkcja SHA-3. G. Bernatek, *Pseudonimizacja danych*, https://rodoradar.pl/pseudonimizacja-danych/, [dostęp: 19.12.2020].

RYSUNEK 15 Dane spseudonimizowane – egzemplifikacja

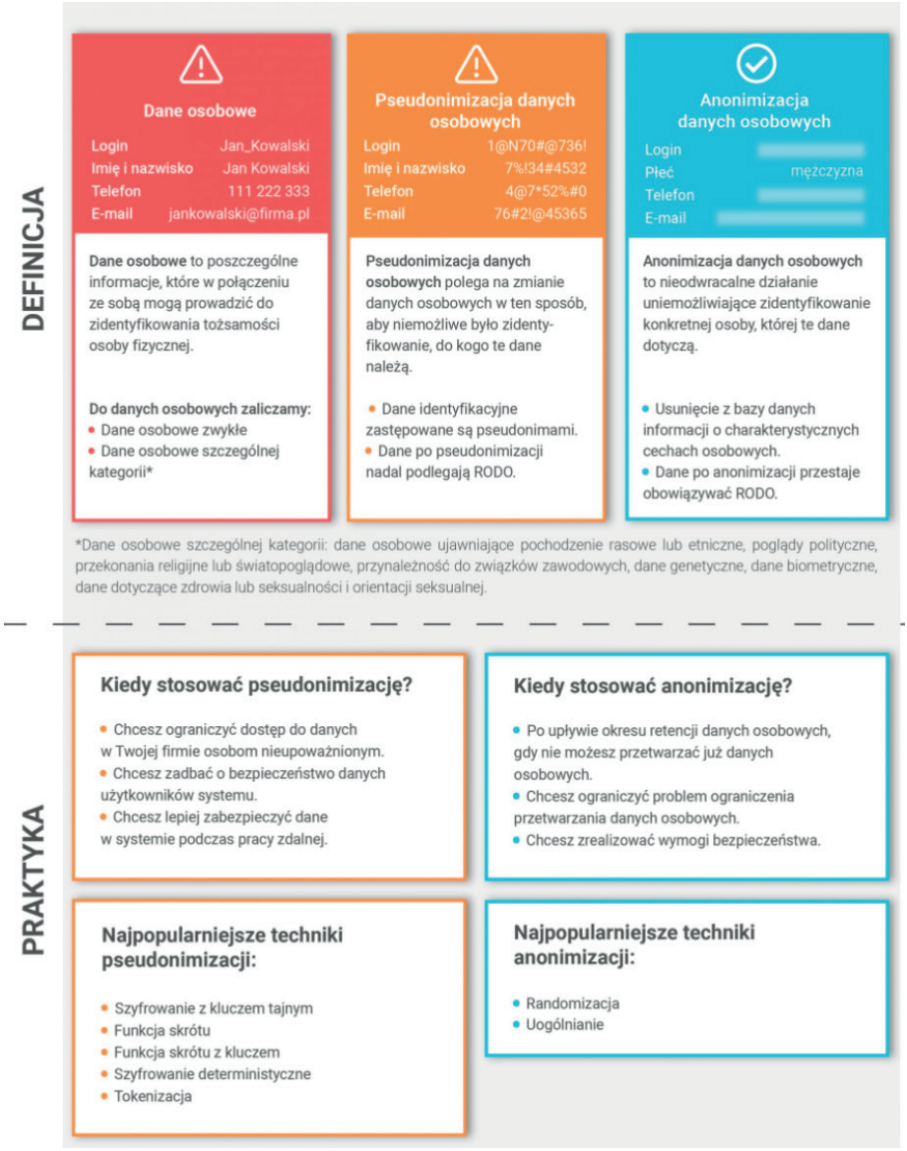


Źródło: W. Wrodarczyk, *Pseudonimizacja danych osobowych w marketingu online*, https://adequate.digital/web-analytics/pseudonimizacja-danych-osobowych-marketingu-online, [dostęp: 17.12.2020]

Należy pamiętać, że pseudonimizacja to nie to samo co anonimizacja, która jest modyfikacją danych uniemożliwiającą identyfikację osoby fizycznej. Pseudonimizacja jest procesem odwracalnym, pośrednim między anonimizacją a przetwarzaniem danych w postaci jawnej. Elementem odróżniającym stosowaną dotychczas anonimizację od pseudonimizacji jest fakt, iż anomizacja pozbawia informację charakteru danych osobowych, natomiast na skutek pseudonimizacji informacje nie tracą przymiotu danych osobowych. W celu zanonimizowania jakichkolwiek danych, musiały być one pozbawione wystarczającej liczby elementów, tak aby nie było już możliwości zidentyfikowania osoby, której dane dotyczą. Dane należy przetwarzać w taki sposób, aby nie istniała już możliwość wykorzystania ich do zidentyfikowania osoby fizycznej za pomocą wszystkich sposobów, jakimi można się posłużyć. Przez proces pseudonimizacji dokonuje się zmodyfikowania danych osobowych w taki sposób, że nie ma możliwości przypisać ich już konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, a co za tym idzie proces ten jest odwracalny. Zwiększa to jedynie bezpieczeństwo informacji, przez co pozostają one według prawa nadal danymi osobowymi. Należy zauważyć, że rozporządzenie traktuje pseudonimizację jako narzędzie pomocnicze[305].

[305] Zob. *RODO dla samorządu i administracji. Wzory dokumentów z objaśnieniami*, K. Czajkowska-Matosiuk, INFOR PL S.A, Warszawa 2018. Por. P. Kowalik, B. Nowakowski, *Zastosowanie ustawy o ochronie danych osobowych w jednostkach sektora publicznego* [w:] A. Gałach, S. Hoc, A. Jedruszczak, K. Kędzierska, P. Kowalik, M. Kuźma, R. Marek, B. Nowakowski, *Ochrona danych osobowych i informacje niejawne w sektorze publicznym*, Wydanie 2, Wydawnictwo C.H. Beck, Warszawa 2015.

RYSUNEK 16 Anonimizacja a pseudonimizacja – dyferencjacje i techniki zastosowań



Źródło: *Anonimizacja i pseudonimizacja danych – techniki ochrony danych*, Newsletter UODO dla Inspektorów Ochrony Danych 2021, nr 4 (25), https://rodoprotektor.pl/anonimizacja-i-pseudonimizacja-danych-osobowych/, [dostęp: 17.12.2020]

Podsumowując, inaczej niż w przypadku anonimizacja, która oznacza nieodwracalne uniemożliwienie zidentyfikowania określonej osoby, dane poddane procesowi pseudonimizacji dalej podlegają ochronie prawnej, w związku z czym administrator danych nie jest zwolniony działania mającego uniemożliwić dostęp do nich osobie nieupoważnionej.

Zwiększenie kontroli podmiotów, których dane są przetwarzane nad swoimi danymi osobowymi

Rozporządzenie wprowadza dwa istotne instrumenty ułatwiające kontrolę podmiotów, których dane podlegają przetwarzaniu, nad swoimi danymi osobowymi. Są to: (1) prawo żądania usunięcia danych, zwane prawem do bycia zapomnianym oraz (2) prawo do przenoszenia danych osobowych. Wprowadzenie prawa do bycia zapomnianym stanowi konsekwencję wyroku wydanego przez Trybunał Sprawiedliwości Unii Europejskiej, w którym uznał, że dyrektywa 95/46/WE umożliwiała osobie, której dotyczą dane, zażądanie od operatora wyszukiwarki internetowej usunięcia z wyświetlanej listy wyników wyszukiwania linków do pewnych stron internetowych ze względu na to, iż życzy ona sobie, aby zawarte na nich informacje zostały „zapomniane". W praktyce uznał on więc prawo obywateli do bycia, w pewnym zakresie, zapomnianym w Internecie[306].

Rozporządzenie wprowadziło zasadę, zgodnie z którą osoba, której dane dotyczą, ma prawo do żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli:

a) osoba ta wycofała zgodę, na podstawie której opierało się przetwarzanie i nie ma innej podstawy do tego, aby dane te nadal przetwarzać,
b) osoba ta wniosła sprzeciw wobec przetwarzania prowadzonego na potrzeby marketingu bezpośredniego, przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym bądź przetwarzania na podstawie prawnie u uzasadnionego interesu realizowanego przez administratora lub stronę trzecią,
c) dane osobowe były przetwarzane niezgodnie z prawem,
d) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator,
e) dane zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego w stosunku do dziecka.

Podkreślenia wymaga, iż administrator danych, do którego zwrócono się z żądaniem usunięcia danych osobowych, jest zobowiązany do niezwłocznego usunięcia danych, przy czym w okolicznościach, w których administrator danych podjąłby decyzję o nieuwzględnianiu wniosku osoby, której dane dotyczą, jest on zobowiązany do udzielenia informacji o powodach podjętego przez siebie rozstrzygnięcia.

Wskazać należy, iż jak podkreśla się w preambule do rozporządzenia, celem wzmocnienia prawa do bycia zapomnianym, administrator danych, który upublicznił dane osobowe, powinien podjąć działania mające na celu poinformowanie administratorów, którzy przetwarzają

[306] Zob. wyrok Trybunału Sprawiedliwości Unii Europejskiej z 13.5.2014 r. (C-131/12, Legalis). Szerzej zob. 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.

takie dane, o usunięciu wszelkich łączy do tych danych, kopii tych danych osobowych lub ich replikacji. Przepisy wskazują, iż spełniając ten obowiązek, administrator danych powinien mieć na uwadze aktualnie dostępną technologię oraz konsekwencje finansowe realizacji tego procesu, a co za tym idzie administrator danych ma obowiązek dokonania wyboru maksymalnie optymalnej technologii, która jednocześnie stanowi gwarancję spełnienia nałożonego obowiązku.

Koncepcja „prawa do bycia zapomnianym" nie jest szeroko analizowana na gruncie polskiej jurysprudencji, co więcej nie jest *sensu stricto* znane polskiemu ustawodawstwu. Najczęściej wskazuje się, że koncepcja ta jest rozwinięciem istniejących w ustawodawstwach państw zachodnich rozwiązań, takich jak prawo do usunięcia danych, które znane jest np. ustawodawstwu francuskiemu (*le droit a l'oubli*), angielskiemu (*right to be forgotten*), włoskiemu (*ildiritto al'oblio*) czy hiszpańskiemu (*el derecho al olvido*)[307]. Żądanie usunięcia określonych informacji nie dotyczy tych danych osobowych, które: (1) umieszczone zostały w przestrzeni publicznej przez samą osobą, której dane są przetwarzane, za jej zgodą, lub gdy osoba zgody nie odwołała; (2) mają charakter oczywiście powszechny (jawny), oraz (3) stanowią dane statystyczne[308].

Prawo to należy rozumieć jako swoiste prawo do odosobnienia (własnego wyboru do alienacji). Niewątpliwą zaletą koncepcji prawa do bycia zapominanym jest możliwość bezpośredniego dochodzenia naruszeń prawa do prywatności przez zainteresowany podmiot, bez potrzeby angażowania organów administracyjnych czy sądów (co znacząco wydłużałoby postępowanie i byłoby dla zainteresowanego kosztowne). Dzięki przyznanemu uprawnieniu jednostka, której prawa zostały naruszone, może sama, za pomocą określonych rozwiązań teleinformatycznych, wnioskować o usunięcie, ukrycie czy zmianę danych. Jest to niewątpliwie jedno z podstawowych narzędzi ochrony prawa do szeroko rozumianej prywatności w przestrzeni cyfrowej[309]. Osobnym zagadnieniem jest fakt, że instytucja ta wprawdzie wyposaża

[307] Instytucja ta stosowana była w celu ochrony byłych skazanych, po odbyciu zasądzonej kary. Polegała na usunięciu, po upływie określonego czasu, niektórych danych dotyczących skazanego oraz popełnionego przez niego czynu, procesu sądowego, odbywania kary itp. Jest zatem zbliżona do regulacji polskich, do jakich w prawie karnym jest zatarcie skazania (art. 106 k.k.). Do pojęcia „prawa do zapomnienia" zbliżona jest instytucja określana prawem do usunięcia danych (lecz nie jest ona z tym pojęciem tożsama). Różni się ona przyznaniem zainteresowanemu podmiotowi roszczenia prawnego. Otóż zainteresowany podmiot ma roszczenie o usunięcie danych, których jest podmiotem, przetwarzanych przez osoby trzecie. Uzasadnienie dla takiego rozwiązania znajduje oparcie w idei, według której każdy, kogo dane są przetwarzane ma prawo do usunięcia takich danych pod pewnymi warunkami, tj. np. jeżeli dane zamieszczone zostały w sposób bezprawny lub jeżeli podmiot danych odwołał wcześniej udzieloną zgodę na ich przetwarzanie. Instytucja prawa do bycia zapomnianym znalazła także swoje oparcie w orzecznictwie. Wielka Izba Trybunału Sprawiedliwości UE 13 maja 2014 roku wydawała wyrok, w którym uznała, że działalność polegająca na zlokalizowaniu informacji opublikowanych lub zamieszczonych w Internecie przez osoby trzecie, indeksowaniu ich w sposób automatyczny, czasowym przechowywaniu takich informacji i wreszcie ich udostępnianiu internautom w sposób uporządkowany zgodnie z określonymi preferencjami, w sytuacji, gdy takie informacje zawierają dane osobowe, należy uznać za „przetwarzanie danych osobowych". Operator wyszukiwarki internetowej będzie zatem „administratorem" odpowiedzialnym za przetwarzanie danych i jest on więc 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 też te informacje nie zostały uprzednio albo jednocześnie usunięte z tych stron internetowych i w odpowiednim przypadku, nawet jeśli ich publikacja na tych stronach jest zgodna z prawem. Kluczową kwestią poruszoną przez TSUE było, czy osoba, której dotyczą dane, ma prawo do tego, aby dotycząca jej informacja nie była już, w aktualnym stanie rzeczy, powiązana z jej imieniem i nazwiskiem poprzez listę wyświetlającą wyniki wyszukiwania mającego za punkt wyjścia to imię i nazwisko, przy czym stwierdzenie, że takie prawo przysługuje, pozostaje bez związku z tym, czy zawarcie na tej liście wyników wyszukiwania danej informacji wyrządza szkodę tej osobie. Zgodnie z wydanym rozstrzygnięciem, w takim stanie faktycznym osoba fizyczna może zażądać, aby ze względu na przysługujące jej uprawnienia, dana informacja nie była już podawana do wiadomości. Zob. wyrok Trybunału Sprawiedliwości Unii Europejskiej z 13 maja 2014 r. (w sprawie C131/12, *Google Spain i Google*, ECLI:EU:C:2014:317, Legalis).

[308] Zob. M. Rojszczak, *Analiza i praktyczne uwagi w zakresie konstrukcji i stosowania prawa do bycia zapomnianym w UE*, Prawo Mediów Elektronicznych 2017, nr 3, s. 30–41.

[309] Szerzej zob. Rezolucja Zgromadzenia Ogólnego ONZ z 16.11.2016 w sprawie prawa do prywatności w erze cyfrowej, sygn. A/C.3/71/L.39/Rev.1. Por. Oświadczenie w sprawie pakietu usług cyfrowych i strategii i w zakresie danych, przyjęte 18 listopada 2021 r., Europejska Rada Ochrony Danych.

bezkosztowo w dodatkowe narzędzie ochrony osoby fizyczne, lecz skutkuje niewątpliwie powstaniem kosztów po stronie podmiotów przetwarzających dane. Procedury związane z rozpatrywaniem wniosków oraz usuwaniem poszczególnych wyników wyszukiwania wiążą się z dodatkowymi kosztami po ich stronie, związanymi z koniecznością stworzenia systemu reagowania na zgłoszenia[310].

Można założyć, że prawo do zapomnienia przeciwdziała bezpodstawnemu gromadzeniu danych osobowych konkretnych osób i zmuszało do usunięcia z obiegu publicznego informacji ich dotyczących – co redukuje zjawisko, jakim jest niekontrolowany handel danymi osobowymi, gromadzonymi przez wyszukiwarki internetowe w ramach tzw. *background screeningu* poprzez wejścia na media społecznościowe, jak Facebook czy Linkedin. Uzyskane w ten sposób dane osobowe (np. dotyczące stanu cywilnego, światopoglądu, hobby, nawyków czy preferencji) w świetle nowych przepisów są bezwartościowe, gdyż z prawnego punktu widzenia nie mogą zostać wykorzystane przez zainteresowane nim pomioty. Nie można jednak zapominać, że nieusunięte informacje stanowią swoistą ingerencję administratora (względnie procesora) w zachowanie oraz status i pozycję osoby, której dane są przetwarzane. Chodzi o informacje powzięte przez otoczenie – rodzinę, znajomych czy kolegów, nie mówiąc już o rodzinie. Poprzez „wymazanie" zamieszczonych na nośnikach cyfrowych danych osobowych osobie stwarza się szansę na wyswobodzenie się od zagrożenia i ingerencji ze strony sfery publicznej. W ten sposób osoba odzyskuje poczucie kontroli nad własnym życiem, bez ingerencji podmiotów trzecich (choć nie można zapomnieć, iż raz powzięte informacje pozostają w pamięci ludzkiej bez względu na fizyczne ich wymazanie z nośników cyfrowych).

Niezależnie od powyższego podkreślić należy, iż prawo do bycia zapomnianym nie ma charakteru absolutnego i podlega istotnym ograniczeniom. Jak słusznie wskazywała Anna Dmochowska (jeszcze przed wejściem w życie omawianych przepisów) „możliwość skorzystania z prawa do bycia zapomnianym będzie wyłączone w zakresie, w jakim przetwarzanie danych jest niezbędne z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego. Będziemy przez to rozumieć przetwarzanie, które odbywa się do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego, lub zgodnie z umową z pracownikiem służby zdrowia. Zaliczymy do tego katalogu również przetwarzanie, które jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki

Por. Komunikat Komisji Europejskiej z 6.05.2015 r. do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, Strategia jednolitego rynku cyfrowego dla Europy, COM (2015) 192 final, CELEX: 52015DC0192; Komunikat Komisji Europejskiej z 25.05.2016 r. do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, „Platformy internetowe i jednolity rynek cyfrowy. Szanse i wyzwania dla Europy", COM(2016) 288 final, CELEX:52016DC0288.

[310] Szerzej zob. P. Brzeziński, B. Opaliński, M. Rogalski, *Gromadzenie i udostępnianie danych telekomunikacyjnych*, Warszawa 2016.

zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa państwa członkowskiego przewidującego odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową. Z prawa do bycia zapomnianym nie będzie można skorzystać także w zakresie, w jakim przetwarzanie danych jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na podstawie prawa Unii lub prawa państwa członkowskiego, jak również, jeżeli będzie to niezbędne do ustalenia, dochodzenia lub obrony roszczeń"[311].

Jeśli zaś chodzi o prawo do przenoszenia danych osobowych regulacja zakłada, że podmiot, którego dane dotyczą, może skorzystać z tego prawa, gdy:

a) wyrażona została zgoda na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów,
b) dane przetwarzane są na podstawie umowy, tj. są 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) wyrażona została wyraźna zgoda na przetwarzanie danych osobowych szczególnych kategorii w jednym lub kilku konkretnych celach,
d) przetwarzanie danych odbywa się w sposób zautomatyzowany[312].

Osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła administratorowi danych. Co ważne, osoba która chce skorzystać z przysługującego jej prawa, może żądać, aby dotyczące jej dane zostały przesłane bezpośrednio do innego administratora danych, oczywiście, jeżeli będzie to technicznie możliwe[313]. Co istotne, omawiane prawo nie znajduje zastosowania w trakcie przetwarzania danych, które jest realizowane w interesie publicznym, jak również w ramach sprawowania władzy publicznej.

Wprowadzenie kontroli na profilowaniem danych

Rozporządzenie definiuje profilowanie jako dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych jednostki (osoby fizycznej). W myśl unijnej regulacji, osoba której dane dotyczą ma prawo do tego, aby nie podlegać decyzji, która opiera się wyłącznie na profilowaniu danymi tej osoby, tj. zautomatyzowanym przetwarzaniu wywołującym wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływającym,

[311] A. Dmochowska, M. Zadrożny, *Unijna reforma ochrony danych osobowych. Analiza zmian*, Warszawa 2016, s. 123.
[312] Szerzej zob. Wytyczne dotyczące prawa do przenoszenia danych 2016/679 z załącznikiem, przyjęte 13 grudnia 2016 r., zmienione i przyjęte 5 kwietnia 2017 r., WP 242 rev.01, Grupa Robocza art. 29.
[313] Art. 20 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 (Dz. Urz. UE L 119 z dn. 4.05.2016, s. 1–88).

w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się (art. 4 RODO)[314].

Profilowanie polega na wykorzystaniu algorytmu, który na bazie wieku, lokalizacji dotychczasowych akcji czy wprowadzanych danych, tworzy profil danej osoby i prognozuje jej przyszłe zachowania. To z kolei umożliwia dopasowanie oferty związanej z preferencjami konkretnego klienta. Przykładowo osoby, które mają cechy X i Y oraz cechę Z zostaną poprzez algorytm połączone z innymi osobami z cechami X i Y, a także cechą Z[315]. Profilowanie może zachodzić tylko na danych przetwarzanych w systemach informatycznych. Profilowanie dotyczy danych osobowych, a nie np. kalkulacji finansowych, czy danych statystycznych, które nie pozwalają zidentyfikować osoby fizycznej. Rezultat profilowania stanowi ocena pozyskanych danych o osobie, której dane przetwarzamy[316].

Kwestia profilowania nabrała szczególnego znaczenia ze względu na rozwój nowych technologii, powstanie Internetu rzeczy, możliwości tworzenia dużych zasobów danych, a przez to, możliwość tworzenia profilów i podejmowania zautomatyzowanych decyzji, co w rozumieniu rozporządzenia może istotnie wpływać lub naruszać prawa i wolności osób fizycznych[317].

RODO dało podstawę prawną do tego, by przeciwdziałać decyzjom, które opierają się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołują wobec osób, których dane dotyczą skutki prawne lub w podobny sposób istotnie na nie wpływają. Bez względu na rodzaj profilowania osoba, której dane dotyczą, ma prawo wnieść sprzeciw. Skutkiem sprzeciwu jest dla administratora zakaz dalszego przetwarzania tych danych osobowych, chyba że wykaże on istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń[318].

Profilowanie samo w sobie nie wiąże się z nałożeniem na administratora lub podmiot przetwarzający dane żadnych dodatkowych obowiązków. RODO nakłada jedynie na administratora

[314] Szerzej zob. 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.

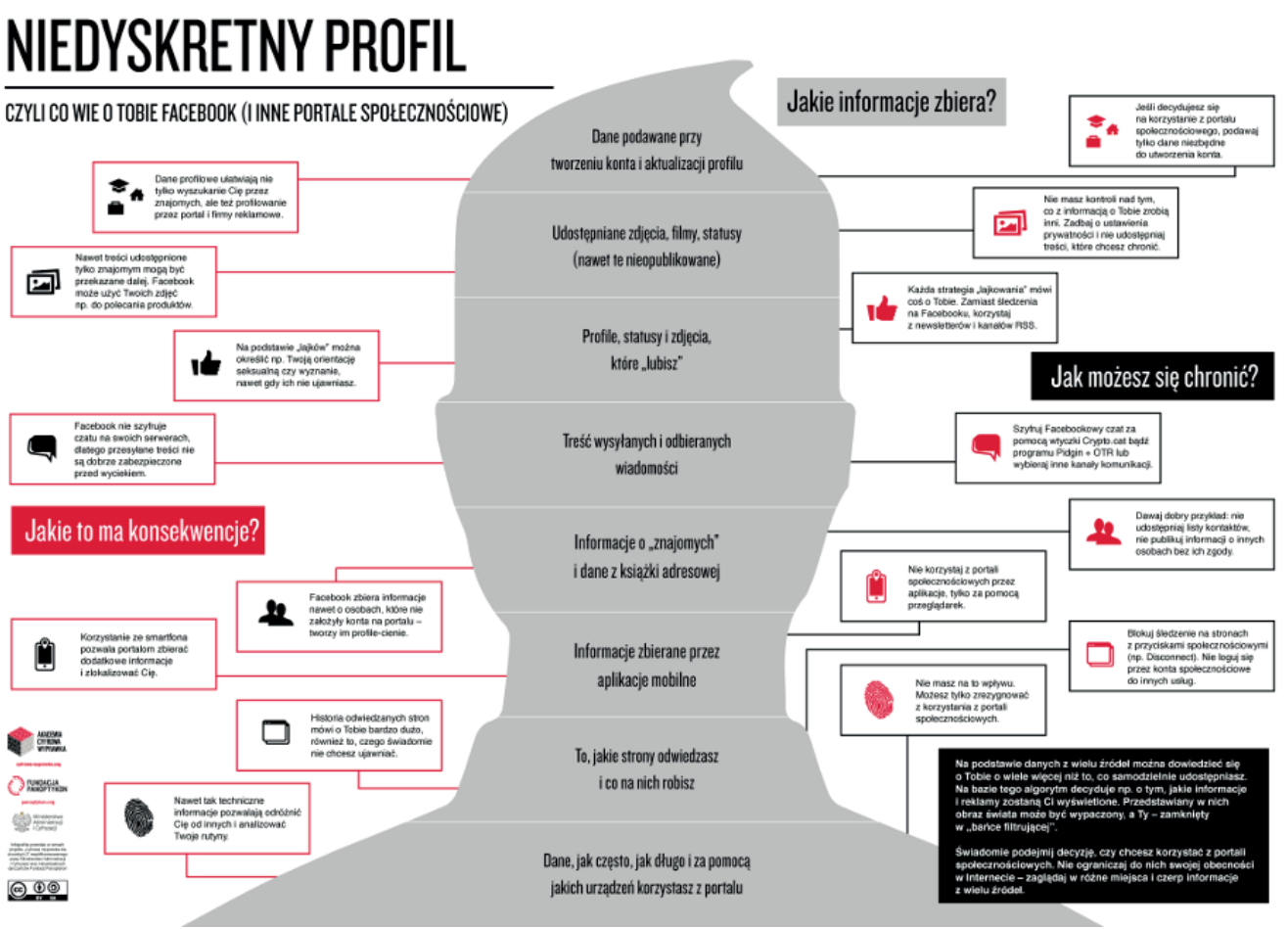
[315] Za pomocą zautomatyzowanego przetwarzania danych osobowych w przeciwieństwie do profilowania nie dokonuje się oceny czynników osobowych podmiotu danych, przez co zautomatyzowane przetwarzane danych osobowych jest pojęciem znacznie szerszym niż „samo". Można powiedzieć, że w praktyce profilowanie stanowi swoistą podkategorię zautomatyzowanego przetwarzania danych. Profilowanie ma miejsce, kiedy administrator dokonuje oceny czynników osobowych jednostki zarówno w obecnej sytuacji, jak i prognoz określonego zachowania na podstawie zautomatyzowanego mechanizmu profilowania. X. Konarski, *Profilowanie danych osobowych na podstawie ogólnego rozporządzenia o ochronie danych osobowych – dotychczasowy i przyszły stan prawny w UE*, Monitor prawniczy 2016, nr 20.

[316] Często zdarza się, że podczas przeglądania oferty sklepu internetowego w oddzielnym panelu wyświetlają się nam propozycje produktów, które powiązane są z wcześniej przeglądanymi przez nas ofertami, np. podczas przeglądania różnych modeli telefonów, w podpowiedziach wyświetlą nam się również oferty pasujących do danego modelu etui, folii czy innych akcesoriów lub też sprzedawca na podstawie dotychczasowych zakupów, będzie mógł przesłać nam spersonalizowane oferty rabatowe. Takie działania można określić jako profilowanie. Profilowanie to jedno z najbardziej popularnych narzędzi marketingowych w e-commerce. Dzięki temu do klienta może dotrzeć zindywidualizowana oferta produktów. Profilowanie spotykamy także przy ocenie ryzyka ubezpieczeniowego lub zdolności kredytowej. Szerzej zob. P. Leja, *Ochrona danych osobowych a Internet rzeczy, profilowanie i repersonalizacja danych*, Prawo Mediów Elektronicznych 2017, nr 3, s. 10–17.

[317] Globalne korporacje teleinformatyczne permanentnie zbierają dane techniczne i użytkowników swoich urządzeń, aplikacji, oprogramowania, sieci. Dane te nazywane są danymi telemetrycznymi. Dzięki telemetrii firmy te mogą nie tylko monitorować, ale również profilować zachowania użytkowników systemu. Często jednak użytkownicy nie mają realnej kontroli nad swoimi danymi, a nawet nie mają świadomości generowania, przetwarzania, utrwalania i wykorzystywania takich danych. Nie są oni informowani, które dane są wykorzystywane i w jakim celu, ani że na podstawie tych danych można spersonalizować każdego użytkownika. Zob. K. Szymielewicz, *Śledzenie i profilowanie w sieci: W czym problem? Co się zmieni w prawie? Jak może wyglądać przyszłość?*, Fundacja Panoptykon, wrzesień 2017, https://panoptykon.org/sites/default/files/publikacje/sledzenie_i_profilowanie_w_sieci_scenariusze_po_reformie_ue_wrzesien_2017.pdf, [dostęp: 30.12.2020].

[318] Szerzej zob. 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

RYSUNEK 17 Profilowanie na przykładzie portali społecznościowych



Źródło: *Jak jesteśmy profilowani w sieci?*, https://cyfrowa-wyprawka.org/lekcja/jak-jestesmy-profilowani-w-sieci, [dostęp: 17.12.2020]

danych obowiązek informacyjny związany z profilowaniem (art. 13 i 14 RODO). Administrator jest zobowiązany poinformować o: (a) tym, że podejmowanie zautomatyzowanych decyzji w ogóle ma miejsce, (b) zasadach, na jakich się odbywa, a także (c) znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą, jak również (d) prawie do wniesienia sprzeciwu. Informacja taka musi zostać przekazana w sposób przejrzysty, konkretny i zrozumiały dla odbiorcy.

Choć rozporządzenie nie wprowadza dosłownie takiego podziału, to profilowanie można podzielić na profilowanie „zwykłe" i profilowanie „szczególne" (zwane też profilowaniem „kwalifikowanym"). Różnica między tymi rodzajami profilowania polega na tym, że w wyniku profilowania szczególnego, wobec danej osoby (której dane osobowe są przetwarzane) zapada jakaś decyzja, która wywołuje wobec tej osoby skutki prawne (np. doprowadza do zawarcia, zmiany lub rozwiązania umowy) lub w podobny sposób istotnie na nią wpływa, natomiast w przypadku profilowania zwykłego takiej decyzji i takiego skutku nie mamy. Jeśli się okaże, że wyłączną podstawą do podejmowania decyzji wobec danej osoby jest zautomatyzowane przetwarzanie danych w postaci profilowania, to konieczne jest spełnienie wymogów z art. 22 RODO. W konsekwencji przepisy wprowadzają konieczną zgodę, gdy dana osoba ma podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu (w tym profilowaniu) i która wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa. Czyli zgoda jest konieczna na profilowanie szczególne. Czasami administrator może się również dopuścić takiego profilowania bez zgody podmiotu danych, jednak wówczas musi być spełniona jedna z dwóch przesłanek:

- jeżeli ta decyzja jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a administratorem;
- jeżeli decyzja jest 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.

Zgoda powinna być wyrażona w drodze jednoznacznej, potwierdzającej czynności, która wyraża odnoszące się do określonej sytuacji dobrowolne, świadome i jednoznaczne przyzwolenie osoby, których dane dotyczą, na przetwarzanie dotyczących jej danych osobowych i która ma na przykład formę pisemnego (w tym elektronicznego) lub ustnego oświadczenia Może to być np. zaznaczenie *checkboxu*, kliknięcie przycisku opisanego jako zgoda lub też napisanie zgody w e-mailu[319].

Przy automatycznym przetwarzaniu administrator wdraża właściwe środki ochrony praw, wolności i uzasadnionych interesów osoby, której dane dotyczą, a co najmniej prawa do uzyskania interwencji, do wyrażenia własnego stanowiska i do zakwestionowania danej

[319] Zob. M. Siwicki, *Ochrona osób fizycznych w związku z przetwarzaniem i swobodnym przepływem danych osobowych*, Państwo i Prawo 2016, nr 3,s. 68–86.

decyzji. O profilowaniu należy informować na etapie zbierania danych osobowych, a także na wniosek osoby[320].

Jednakowoż, omawiane prawo nie znajdzie zastosowania, w przypadku gdy decyzja oparta jest jedynie na zautomatyzowanym przetwarzaniu jest: (a) niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a administratorem, (b) dopuszczalna zgodnie z prawem unijnym 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) oparta jest na wyraźnej zgodzie osoby, której dane dotyczą.

Konkludując, zawsze gdy efektem profilowania będzie podjęcie decyzji w indywidualnej sprawie, a dodatkowo przedmiotowe przetwarzanie będzie wywoływało skutki prawne wobec osoby, której dane dotyczą, lub w podobny sposób istotnie na nią wpływało, administrator danych ma prawny obowiązek uzyskania wyraźnej zgody na przetwarzanie danych. Przy czym decyzje, które zostały oparte na profilowaniu, i wywołują wobec osoby, której dane dotyczą, skutki prawne, nie mogą opierać się na tzw. danych wrażliwych, czyli szczególnych kategoriach danych osobowych. Wyjątkiem od tej zasady jest sytuacja, gdy podmiot, którego dane dotyczą, wyraził wyraźną zgodę na przetwarzanie tych danych osobowych lub przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym. Nadto przetwarzanie nie powinno dotyczyć dzieci, jak również nie może prowadzić do dyskryminacji z uwagi na pochodzenie etniczne lub rasowe, poglądy polityczne, wyznanie lub przekonania, przynależność do związków zawodowych, stan zdrowotny lub genetyczny, orientację seksualną lub skutkujący środkami mającymi taki efekt. To na administratorze ciąży obowiązek wprowadzenia takich metod profilowania, które pozwolą uzyskać pewność eliminacji ewentualnych błędów.

Rozszerzenie obowiązku informacyjnego w trakcie zbierania danych osobowych

Rozporządzenie wprowadziło wymóg przejrzystości informowania oraz jasności komunikowania osobie, której dane dotyczą, jej praw (obowiązek zapewnienia dostatecznego poziomu informacyjnego). Rozporządzenie wprowadziło w motywie 58 zasadę przejrzystości, która jest definiowana jako zwięzłość, dostępność, czytelność wszelkich informacji przekazywanych podmiotowi danych lub ogółowi odbiorców (szczególnie dzieciom), wynikającą również z jednoznacznego języka, ewentualnie z formy graficznej. Podkreśla się szczególne znaczenie takiej klarownej, przejrzystej informacji, gdy stopień skomplikowania technologicznego utrudnia podmiotowi danych rozpoznanie, przez kogo i w jakim celu jego dane osobowe są gromadzone. Postulaty te zostały zmaterializowane w art. 12 rozporządzenia. W przypadku klauzul informacyjnych przy zbieraniu danych (art. 13 i 14 RODO), w odniesieniu do wniosku podmiotu danych o udzielenie informacji (art. 15 RODO), w razie automatycznego podejmowania

[320] Jeżeli profilowanie odbywa się w celu marketingu bezpośredniego (który do wejścia w życie RODO stanowił tzw. usprawiedliwiony prawnie cel przetwarzania, zaś w rozporządzeniu jest teraz mowa o tzw. celach wynikających z uzasadnionych interesów administratora danych) można zgłosić sprzeciw w związku z takim przetwarzaniem. Zob. Opinia 06/2014 w sprawie pojęcia uzasadnionych interesów administratora danych zawartego w art. 7 dyrektywy 95/46/WE, WP 217, przyjęta 9 kwietnia 2014 r, Grupa robocza art. 29.

przez administratora decyzji mającej istotny wpływ na podmiot danych, w tym profilowania (art. 22 RODO), oraz w przypadku informowania podmiotu danych o naruszeniach ochrony jego danych (art. 34 RODO).

Zgodnie z art. 12 rozporządzenia 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. Należy udzielić osobie, której dane dotyczą, wszelkich informacji, o których mowa w art. 13 i 14 rozporządzenia. Informacji udziela się na piśmie lub w inny sposób, w tym w stosownych przypadkach – elektronicznie. Jeżeli osoba, której dane dotyczą, tego zażąda, informacji można udzielić ustnie, o ile innymi sposobami potwierdzi się tożsamość osoby, której dane dotyczą. Administrator ułatwia osobie, której dane dotyczą, wykonanie praw przysługujących jej na mocy art. 15–22 rozporządzenia. W przypadkach, o których mowa w art. 11 ust. 2 RODO, administrator nie może odmówić podjęcia działań na żądanie osoby której dane dotyczą, czyli pragnącej wykonać prawa przysługujące jej na mocy art. 15–22 RODO, chyba że wykaże, iż nie jest w stanie zidentyfikować osoby, której dane dotyczą. Administrator bez zbędnej zwłoki – a w każdym razie w terminie miesiąca od otrzymania żądania – udziela osobie, której dane dotyczą, informacji o podjętych działaniach. W razie potrzeby termin ten można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań. W terminie miesiąca od otrzymania żądania administrator informuje osobę, której dane dotyczą o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia. Jeśli osoba, której dane dotyczą, przekazała swoje żądanie elektronicznie, w miarę możliwości informacje także są przekazywane elektronicznie, chyba że osoba, której dane dotyczą, zażąda innej formy. Jeżeli administrator nie podejmuje działań w związku z żądaniem osoby, której dane dotyczą, to niezwłocznie – najpóźniej w terminie miesiąca od otrzymania żądania – informuje osobę, której dane dotyczą, o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem. Informacje podawane w przypadku zbierania danych od osoby, której dane dotyczą oraz w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą, są wolne od opłat. Jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, administrator może pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań albo odmówić podjęcia działań w związku z żądaniem. Obowiązek wykazania, że żądanie ma ewidentnie nieuzasadniony lub nadmierny charakter, spoczywa na administratorze. Informacje, których udziela się osobom, których dane dotyczą, można opatrzyć standardowymi znakami graficznymi, które w widoczny, zrozumiały i czytelny sposób przedstawiają sens zamierzonego przetwarzania. Jeżeli znaki te są przedstawione elektronicznie, muszą się nadawać do odczytu.

Przepis artykułu 12 rozporządzenia stanowi wspólny mianownik dla przekazania podmiotowi danych informacji o ich zebraniu przez administratora, prawa do dostępu do przetwarzanych danych, prawa do usunięcia danych („prawa do bycia zapomnianym"), sprzeciwu wobec

przetwarzania danych, powiadomienia podmiotu danych o naruszeniu ich ochrony (a więc obowiązków i praw określonych w art 13–22 oraz 23 RODO). Obowiązek informacyjny, podczas zbierania danych, został znacznie poszerzony o informowanie o: (a) Inspektorze Ochrony Danych, (b) nazwie i danych kontaktowych przedstawiciela jeżeli istnieje, (c) podstawę prawną przetwarzania, (d) prawnie uzasadniony interes administratora jeżeli na tej podstawie odbywa się przetwarzanie, (e) informacje o zamiarze przekazywania danych do państwa trzeciego, (f) okresie przez, który dane osobowe będą przechowywane bądź kryteria ustalania tego okresu, (g) profilowaniu, (h) o prawie wniesienia skargi do organu nadzorczego, (i) w przypadku istnienia obowiązku podania danych osobowych: wskazanie ewentualnych konsekwencji niepodania danych, (j) prawach osoby, której dane dotyczą (tj. prawie do usunięcia danych, ograniczenia przetwarzania, prawie przenoszenia danych, prawie do cofnięcia zgody gdy osoba, której dane dotyczą wyraża zgodę na przetwarzanie danych).

RODO określa formę komunikacji, tryb i terminy wykonywania obowiązkowi i egzekwowania praw, w tym np. częstotliwość i ewentualną odpłatność, dopuszczając rozmaite formy przekazania wymaganych informacji o przetwarzaniu danych, nie tylko pisemną, lecz także inne, w tym elektroniczne, a także formę ustną, gdy takiej życzy sobie wnioskodawca. Udzielenie informacji wymaga potwierdzenia tożsamości podmiotu danych. Rozporządzenie wymaga zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formy oraz jasnego i prostego języka, zwłaszcza gdy informacje są kierowane do dziecka. Informacyjne obowiązki można spełnić poprzez zastosowanie klauzul przy zbieraniu danych w formie standardowych ikon, które czytelnie przedstawiają sens planowego przetwarzania danych (ikony przedstawione elektronicznie muszą się nadawać do odczytu). W tym celu skuteczną formą może być podpis na stosowanym przez administratora formularzu, zaznaczenie okienka przy klauzuli na stronie internetowej lub taka sekwencja komunikatów na stronie internetowej, w której przejście do informacji o produktach wymaga zapoznania się z informacjami o przetwarzaniu danych. Wymagane informacje mogą być również przekazane w rozmowie telefonicznej prowadzonej przez *call center* administratora danych. Dowodem przekazania informacji może być nagranie rozmowy lub wdrożenie w regulacjach wewnętrznych administratora danych scenariusza rozmowy telefonicznej zawierającego właściwą klauzulę. Warunkiem prawidłowości spełnienia obowiązku informacyjnego jest skierowanie i przekazanie informacji wprost osobie, której dane dotyczą. Wyklucza to formy takie, jak tablica ogłoszeń czy prasa lub Internet[321].

Zmiany wymagały wymiany wszelkich formularzy dotyczących zgody na przetwarzanie danych osobowych, zarówno papierowych jak i elektronicznych. Nowe klauzule zgody, formularze czy tzw. *check boxy* zdecydowanie poszerzyły swoją objętość. Dla mniejszych jednostek organizacyjnych skutkowało to koniecznością wniesienia znacznego nakładu zasobów

[321] Komisja Europejska jest uprawniona do określenia, jakie informacje należy przedstawić za pomocą ikon i do ustandaryzowania tych symboli (co wynika wprost z art. 12 ust. 7 i 8 rozporządzenia. Zob. *Obowiązek informacyjny w praktyce – po co, kiedy i gdzie?*, GDPR.PL, https://gdpr.pl/obowiazek-informacyjny-w-praktyce-po-co-kiedy-i-gdzie, [dostęp: 29.11.2021].

przy pozyskiwaniu zgód na przetwarzanie danych osobowych[322]. Jednocześnie należy wskazać, iż osoba, której dane dotyczą, może wnosić o wszczęcie postępowania administracyjnego przez organ ochrony danych w przypadku ignorowania lub niewystarczającej skuteczności jej praw, których realizacji się domaga[323]. Jeżeli administrator nie podejmuje działań, o które wnosi podmiot danych, jest zobowiązany niezwłocznie, najpóźniej w terminie miesiąca od otrzymania żądania, zawiadomić wnioskodawcę o powodach braku działań i o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem (art. 12 ust. 4 RODO). Rozporządzenie zapewniło elastyczność formy składania wniosków i odpowiedzi na nie – mogą być przekazywane pisemnie lub w innych formach. Również elektronicznie – i ta forma determinuje też, w miarę możliwości, elektroniczne przekazanie odpowiedzi przez administratora, o ile wnioskodawca nie wskaże innej formy przekazania mu informacji (art. 12 ust. 1 i 3 RODO). Administrator jest jednak odpowiedzialny za wdrożenie procedur zapobiegających udzieleniu informacji i podejmowaniu działań na wniosek osoby nieuprawnionej, która posługuje się tożsamością podmiotu danych, np. przesyła wniosek z adresu e-mail założonego przez siebie na nazwisko podmiotu danych. Pochopne udzielenie informacji lub uwzględnienie żądania pochodzącego rzekomo od podmiotu danych mogłoby prowadzić nie tylko do naruszenia ochrony danych (*fraud'u*), lecz także umożliwić sprawcy kradzież tożsamości lub wyrządzić inną szkodę (np. ułatwić *phishing* – oszustwo z wykorzystaniem posiadanych informacji o osobie fizycznej, w celu podszycia się pod nią i wyłudzenia danych umożliwiających odkrycie loginów i haseł do poczty elektronicznej lub bankowości internetowej).

Należy przyjąć, że w razie braku możliwości identyfikacji wnioskodawcy art. 11 ust. 2 rozporządzenia wyłącza stosowanie art. 15–20 RODO ale nie wyłącza stosowania art. 21 RODO. W takiej sytuacji nie jest zatem dopuszczalne np. przekazanie niezidentyfikowanemu wnioskodawcy informacji o podmiocie danych ani korekta tych danych – z uwagi na groźbę nieuprawnionego uzyskania informacji chronionych lub np. zmianą adresu do korespondencji i następnie przesyłaniem jej przestępcy. Jednocześnie, z uwagi na fakt, że art. 21 RODO nie ulega bezwzględnemu wyłączeniu, dopuszczalne jest uwzględnienie np. sprzeciwu marketingowego, gdy nie grozi to ujawnieniem danych osobowych i okoliczności nie sugerują usiłowania nadużycia lub przestępstwa. Bez względu na rozbieżności stanowisk doktryny, rozważenie konkretnych przypadków może przysparzać trudności, ze wszystkim z tego tytułu płynącymi konsekwencjami prawnymi.

Wprowadzenie zasad dotyczących przetwarzania danych dzieci

Motyw 38 preambuły RODO stanowi, 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. Taka szczególna ochrona powinna

[322] Zob. *Prawo procesowe administracyjne*, red. R. Hauser, A. Wróbel, Z. Niewiadomski, wyd. 3, Warszawa 2017.
[323] Zob. M. Krzysztofek, *Ochrona danych osobowych w Unii Europejskiej po reformie. Komentarz do rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679*, Warszawa 2016.

mieć zastosowanie przede wszystkim do wykorzystywania danych osobowych dzieci do celów marketingowych lub do tworzenia profili osobowych lub użytkownika oraz do zbierania danych osobowych dotyczących dzieci, gdy korzystają one z usług skierowanych bezpośrednio do nich. Zgoda osoby sprawującej władzę rodzicielską lub opiekę nie powinna być konieczna w przypadku usług profilaktycznych lub doradczych oferowanych bezpośrednio dziecku. Odniesienia do szczególnej ochrony danych osobowych dzieci można znaleźć również w dalszych motywach RODO. Przykładowo zasada przejrzystości, którą powinni kierować się administratorzy danych, wymaga, aby wszelkie informacje kierowane do ogółu społeczeństwa lub osoby, której dane dotyczą, były zwięzłe, łatwo dostępne i zrozumiałe, oraz by były formułowane jasnym i prostym językiem, a w stosownych przypadkach dodatkowo wizualizowane (informacje te mogą być przekazywane w formie elektronicznej, np. za pomocą strony internetowej).

Norma ogólna RODO stanowi, iż przetwarzanie danych osobowych zwykłych jest dopuszczalne pod warunkiem spełnienia przez administratora danych co najmniej jednej z sześciu (pięciu – w przypadku organów publicznych w ramach realizacji ich zadań) równorzędnych przesłanek określonych w art. 6 rozporządzenia. Wykazanie przez administratora danych istnienia prawnej podstawy przetwarzania jest więc warunkiem wyjściowym jego zgodności z prawem (zasada legalności). Treść zgody na przetwarzanie danych jako oświadczenia woli podlega wykładni według przepisów prawa cywilnego. Jednoznaczna zgoda może zostać udzielona w sposób wyraźny – wprost przez deklarację ustną, pisemną, wybór opcji w formularzu na stronie internetowej, lub dorozumiany – gdy wynika ona z określonych okoliczności[324]. Podstawę prawną przetwarzania musi wykazać każdy administrator zbierający dane, udostępniający je innemu administratorowi oraz administrator, któremu zostały one udostępnione. Kategorie danych określone w art. 9 i 10 rozporządzenia (dane wrażliwe) ze względu na szczególne znaczenie dla prawa do prywatności podlegają znacznie bardziej rygorystycznym zasadom. Różnica między przesłankami dopuszczalności przetwarzania danych zwykłych i wrażliwych wynika z odwrócenia podstaw przetwarzania.

Poziom ochrony danych osobowych dzieci jest zatem znacznie podwyższony w stosunku do przetwarzania danych w przypadku dorosłych. Uzasadnieniem jest oczywiście niższa świadomość ryzyka, konsekwencji, zabezpieczeń i praw przysługujących im w związku z przetwarzaniem

[324] Do dobrowolności zgody – na przykładzie przetwarzania przez pracodawców danych biometrycznych pracowników – odniosła się ponadto Grupa Robocza Art. 29 w dokumencie roboczym w sprawie biometrii z 1.08.2003 r., w którym uznała przyjęcie zgody podmiotu danych jako podstawy przetwarzania danych biometrycznych wyłącznie pod warunkiem pełnej swobody udzielenia zgody i braku konsekwencji odmowy. Dobrowolność zgody, która jest warunkiem jej ważności, oznacza, że odmowa zgody nie może powodować negatywnych konsekwencji dla podmiotu danych. Przez negatywne konsekwencje nie należy jednak rozumieć utraty korzyści, np. gdy w standardowych relacjach handlowych są one powiązane ze zgodą na marketing, a więc gdy udzielony rabat jest ceną płaconą przez sklep klientowi za możliwość prowadzenia. Przykładowo niedopuszczalne jest uzależnianie wykonania umowy, w tym świadczenia usługi, od zgody na przetwarzanie danych w celu prowadzenia marketingu. Podobnie wyrażenie zgody blankietowej jest bezskuteczne – zgoda nie może się odnosić do nieokreślonego zakresu danych oraz do nieoznaczonego celu. Dopuszczalne jest ograniczenie zgody przez odniesienie jej wyłącznie do wskazanych danych lub celów przetwarzania, operacji wykonywanych na danych osobowych, wskazanego okresu bądź terytorium lub przez uzależnienie zgody od warunku. Jednak w praktyce większości instytucji, które przetwarzają wiele kategorii danych w zróżnicowanych celach, stosowanie takiego zróżnicowania nie jest technicznie możliwe i konieczne jest przyjęcie standardowych oświadczeń o zgodzie na przetwarzanie danych. Należy ponadto zweryfikować, czy po wyrażeniu zgody przez podmiot danych nie nastąpiła zmiana okoliczności, do których zgoda się odnosiła. Zmiana celu i zakresu przetwarzania, jeżeli zgoda ma być jego podstawą, wymaga ponownego uzyskania przez administratora zgody podmiotu danych odnoszącej się do zmodyfikowanych okoliczności. Zob. Dokument Grupy Roboczej Art. 29 nt. biometrii, WP80, przyjęty w dniu 1 sierpnia 2003 r. Wymagania dotyczące przetwarzanie danych biometrycznych w świetle także w innych dokumentach Grupy Roboczej Art. 29, w tym m.in.: (1) opinii 4/2007 w sprawie pojęcia danych osobowych, WP 136, przyjętej 20 czerwca 2007 r., (2) opinii 02/2012 w sprawie systemów rozpoznawania twarzy w usługach online i usługach komórkowych, WP 192, przyjętej w dniu 22 marca 2012 r., (3) opinii 3/2012 w sprawie zmian sytuacji w dziedzinie technologii biometrycznych, WP 193, przyjętej 27 kwietnia 2012 r.

danych osobowych. Zważywszy, że dzieci zasługują na szczególną ochronę, wszelkie informacje i komunikaty powinny być sformułowane tak jasnym i prostym językiem, by dziecko mogło go bez trudu zrozumieć. Ta szczególna ochrona obejmuje przede wszystkim wykorzystywanie danych osobowych do celów marketingowych lub do tworzenia profili osobowych lub użytkownika oraz do świadczenia usług skierowanych bezpośrednio do dzieci (motyw 38 rozporządzenia). Co najważniejsze, profilowanie nie może dotyczyć dzieci, przy czym przepisy rozporządzenia podkreślają w preambule, że zgoda osoby sprawującej władzę rodzicielską lub opiekę nie powinna być konieczna w przypadku usług profilaktycznych lub doradczych oferowanych bezpośrednio dziecku.

Zasadniczo zgodę na przetwarzanie danych osobowych dziecka wyrażają jego rodzice lub prawni opiekunowie. Jednakże w przypadku usług społeczeństwa informacyjnego[325] zdarza się, że są one kierowane bezpośrednio do dzieci. Ma to miejsce np. w sytuacji, gdy dziecko może poprzez własne działanie stać się użytkownikiem takich usług (np. samodzielne utworzenie konta w serwisie społecznościowym). Jeżeli dziecko nie ukończyło 16 lat, takie przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy zgodę wyraziła lub zaaprobowała ją osoba sprawująca władzę rodzicielską lub opiekę nad dzieckiem oraz wyłącznie w zakresie wyrażonej zgody.[326] Oznacza to, że osoba, która przekroczyła ten wiek, może samodzielnie wyrazić zgodę bez potrzeby jej potwierdzania przez rodziców czy opiekunów prawnych. RODO stanowi, że państwa członkowskie mogą przewidzieć w swoim prawie niższą granicę wiekową, która musi wynosić co najmniej 13 lat. W pierwotnym projekcie polskiej ustawy o ochronie danych osobowych znajdowały się przepisy, które obniżały ten wiek do lat 13, ale po przeprowadzonych konsultacjach utrzymano granicę 16 lat. Jednocześnie RODO wymaga, aby administrator podjął starania, uwzględniając dostępną technologię, by zweryfikować, czy osoba sprawująca władzę rodzicielską lub opiekę nad dzieckiem wyraziła zgodę lub ją zaaprobowała, a zatem to czy osoba sprawująca władzę rodzicielską lub opiekę nad dzieckiem wyraziła lub zaaprobowała zgodę na przetwarzanie danych dziecka poniżej określonego progu wieku, podlega weryfikacji przez administratora. Ze względu na charakter usług społeczeństwa informacyjnego zgoda na ich świadczenie jest udzielana w sieci, więc to, czy oświadczenie zostało złożone rzeczywiście przez uprawnioną osobę jest często uprawdopodobnione, a nie udowodnione. Przepis wymaga więc podjęcia w tym celu rozsądnych starań, uwzględniających dostępną technologię. W praktyce narzędzia opracowane przez administratorów będą najpewniej wynikać z dostępnych narzędzi informatycznych oraz specyfiki konkretnych administratorów. Przykłady stosowanych rozwiązań

[325] Usługi społeczeństwa informacyjnego to wszystkie usługi normalnie świadczone za wynagrodzeniem, na odległość, drogą elektroniczną i na indywidualne żądanie odbiorcy usług (art. 4 pkt 25 rozporządzenia). To zatem liczne i dynamicznie rosnące kategorie usług, takich jak: usługi finansowe on-line (bankowość internetowa, sprzedaż ubezpieczeń on-line), sprzedaż innych usług, np. turystycznych, sklepy internetowe, np. sprzedaż książek i muzyki w księgarniach internetowych, sprzętu elektronicznego, ubrań, kosmetyków, prenumerata gazet on-line, sprzedaż aplikacji mobilnych. Załącznik I dyrektywy 2015/1535 precyzuje przykładowy wykaz usług nienależących do tej kategorii ze względu na to, że nie są świadczone „na odległość", np. wgląd do elektronicznego katalogu w sklepie przy fizycznej obecności klienta, ze względu na to, że nie są świadczone „drogą elektroniczną", np. bankomaty i biletomaty, oraz ze względu na to, że nie są świadczone „na indywidualne żądanie odbiorcy usług", lecz przeznaczone do odbioru przez nieograniczoną liczbę odbiorców, np. transmisja programu telewizyjnego. Zob. 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 (Tekst mający znaczenie dla EOG), (Dz.Urz. UE L z 17.09.2015, s. 1–15. Por. Wytyczne 6/2020 w sprawie współzależności pomiędzy dyrektywą PSD2 a RODO, wersja 2.0, przyjęte 15 grudnia 2020 r., Europejska Rada Ochrony Danych.

[326] Zgodnie z art. 8 rozporządzenia jeżeli zastosowanie ma art. 6 ust. 1 lit. a (osoba, której przetwarzane są dane wyraziła na to zgodę), w przypadku usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku, zgodne z prawem jest przetwarzanie danych osobowych dziecka, które ukończyło 16 lat.

to: blokada konta na portalu społecznościowym do czasu potwierdzenia wieku przez przesłanie w e-mailu skanu dowodu tożsamości albo potwierdzenie zgody z adresu e-mail rodzica lub poprzez rozmowę telefoniczną.

Szczególne uprawnienia dotyczą możliwości sprostowania danych oraz skorzystania z prawa do „bycia zapomnianym", w przypadku gdy osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie jeszcze jako dziecko. Ma ona prawo do tego, by jej dane osobowe zostały usunięte i przestały być przetwarzane, jeżeli:

- dane te nie są już niezbędne do celów, dla których były zbierane lub przetwarzane,
- cofnęła zgodę lub jeżeli wniosła sprzeciw wobec przetwarzania danych osobowych jej dotyczących, lub gdy przetwarzanie jej danych nie jest zgodne z RODO.

Prawo to ma szczególne znaczenie w przypadkach, gdy osoba, której dane dotyczą, wyraziła zgodę jako dziecko, gdy nie była w pełni świadoma ryzyka związanego z przetwarzaniem, a w późniejszym czasie chciała usunąć takie dane osobowe. Osoba, której dane dotyczą, ma możliwość wykonać to prawo, nawet po utraceniu statusu dziecka. Niemniej dalsze zatrzymywanie danych osobowych może być uznane za zgodne z prawem, jeżeli jest to niezbędne: (a) do korzystania z wolności wypowiedzi i informacji, (b) do wywiązania się z obowiązku prawnego, (c) do wykonania zadania realizowanego w interesie publicznym lub (d) w ramach sprawowania władzy publicznej powierzonej administratorowi, z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego, do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych bądź do celów statystycznych lub do ustalenia, dochodzenia bądź obrony roszczeń.

Doprecyzowanie zasad dotyczących transferu danych do państw trzecich

Obostrzenia przy zagranicznych transferach danych osobowych były przewidziane już w polskiej ustawie o ochronie danych osobowych z 1997 roku. RODO wprowadziło jednak dużo istotnych modyfikacji, a przekazywanie danych osobowych do państw trzecich stało się znacznie bardziej wymagającym zadaniem. Mimo, że państwa europejskie szczycą się najbardziej zaawansowanymi regulacjami prawnymi, chroniącymi prywatność[327], to jednak poziom technologizacji i globalizacji, nie pozwala na zamknięcie się w bezpiecznej bańce obszaru bezpiecznego przetwarzania. Wprowadzenie obostrzeń przy przekazywaniu danych do państw trzecich ma służyć utrzymaniu skutecznej ochrony mieszkańców Europejskiego Obszaru Gospodarczego (EOG)[328], również poza obszarem obowiązywania RODO[329].

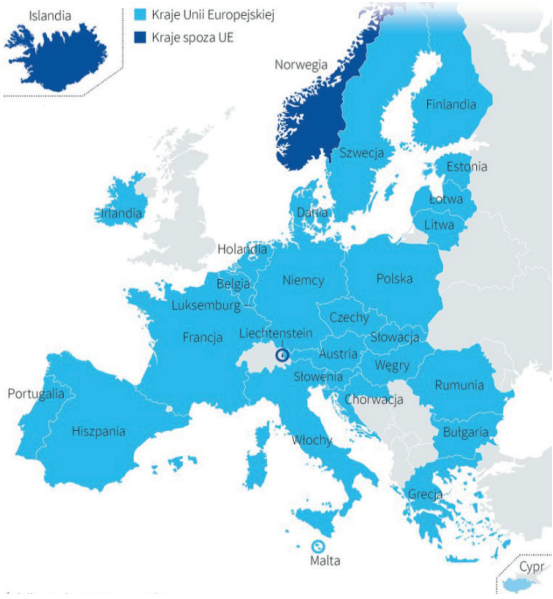
[327] Zob. m.in. (a) Rezolucja Zgromadzenia Ogólnego ONZ z 16.11.2016 w sprawie prawa do prywatności w erze cyfrowej, sygn. A/C.3/71/L.39/Rev.1, (b) Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, 23.09.1980, C(80)58/FINAL, (c) Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, 11.07.2013, C(2013)79, (d) The OECD Privacy Framework, OECD 2013.

[328] Zob. Przyszłość prywatności: Wspólny wkład do Konsultacji Komisji Europejskiej w sprawie ram prawnych dla podstawowego prawa do ochrony danych osobowych, WP 168, Grupa robocza art. 29.

[329] Szerzej na temat zakresu obowiązywania RODO zob. Wytyczne 3/2018 w sprawie terytorialnego zakresu stosowania RODO (artykuł 3), wersja 2.0, przyjęte 12 listopada 2019 r., Europejska Rada Ochrony Danych.

System jest tak skonstruowany, że preferuje obszar UE i EOG przy przetwarzaniu danych osobowych[330]. Sytuacja transferu danych, zgodnie z RODO, ma miejsce po pierwsze w ramach czynności operacyjnej przekazywania danych, po drugie w sytuacji relacyjnej z tzw. „państwem trzecim". Przy czym rozporządzenie w ogóle nie wprowadza ani definicji państwa trzeciego, ani definicji transferu danych. Przyjmuje się jednak, że sytuacja transferu danych powinna być rozumiana bardzo szeroko. Obszarem wyjściowym jest EOG. obiegowa opinia, że państwo trzecie, to państwo, które nie jest w UE – nie jest prawdą. Konieczne zatem jest ustalenie czy państwo, do którego ma miejsce transfer danych osobowe, jest tzw. państwem trzecim. I tak będzie to każde państwo, które nie wchodzi w skład Europejskiego Obszaru Gospodarczego. Tu należy jedynie przypomnieć, że obszar EOG integruje państwa Unii Europejskiej z Islandią, Liechtensteinem i Norwegią[331].

RYSUNEK 18 Kraje Europejskiego Obszaru Gospodarczego



Źródło: *Europejski Obszar Gospodarczy (EOG), Szwajcaria i kraje północy*, Parlament Europejski https://www.europarl.europa.eu/ftu/pdf/pl/FTU_5.5.3.pdf, [dostęp:17.12.2020]

[330] To oprócz bezpieczeństwa danych ma jeszcze jedną dodatkową korzyść dla całej UE bowiem wymusza budowanie centrów danych i serwerowni w Europie. Szerzej zob. M. Polok, *Bezpieczeństwo danych osobowych*, Warszawa 2016.

[331] Od 1 stycznia 2021 roku Wielka Brytania jest traktowana na takich samych zasadach, jak każde inne państwo trzecie. (do czasu podjęcia przez Komisję decyzji o uznaniu Wielkiej Brytanii, za państwo dające odpowiedni stopień ochrony danych). Oznacza to, że wszystkie transfery danych do tego państwa muszą spełniać dodatkowe wymogi dotyczące przekazywania danych do państw trzecich lub organizacji międzynarodowych, które zostały określone w rozdziale V RODO. Do czasu wydania przez KE stosownej decyzji umożliwiającej legalność transferów danych do Wielkiej Brytanii każdy administrator danych lub podmiot przetwarzający, którzy przekazują dane do Wielkiej Brytanii „w okresie przejściowym" powinien: (a) zidentyfikować, jakie dane, w jakich celach i na jakiej podstawie prawnej są przekazywane, (b) zdecydować, czy te transfery będą kontynuowane, (b) wybrać i wdrożyć odpowiedni mechanizm, bądź podstawę prawną umożliwiającą przekazywanie danych, (c) w razie potrzeby zmodyfikować wewnętrzną dokumentację przetwarzania danych, w tym rejestr czynności przetwarzania, klauzule informacyjne, istniejące wiążące reguły korporacyjne. Zob. *Prezes UODO wyjaśnia, jak przekazywać dane osobowe z Polski do Wielkiej Brytanii na wypadek Brexitu*, https://uodo.gov.pl/pl/138/665, [dostęp: 06.12.2020]. Zob. też. Oświadczenie dotyczące końca okresu przejściowego Brexit, przyjęte 15 grudnia 2020 r., Europejska Rada Ochrony Danych. Por. 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 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.

Transfer dotyczy każdej sytuacji, kiedy przekazywane dane osobowe z EOG na zewnątrz, mają charakter powtarzalny, wielokrotny i złożony (jak na przykład korzystanie z serwerów zlokalizowanych na terenie państwa trzeciego, globalny outsourcing wsparcia IT czy korzystanie z różnego rodzaju komunikatorów transferujących dane poza EOG), jak i przypadków incydentalnych (np. elektroniczne udostępnienie dokumentu z danymi osobowymi komuś przebywającemu poza EOG)[332].

Przekazywanie danych osobowych do państw trzecich może nastąpić wyłącznie pod warunkiem spełnienia określonych warunków, wskazanych w rozdziale V. RODO wprowadza standard kilku następujących po sobie kaskadowo kroków. Dwa pierwsze to identyfikacja obszaru (kraju) do którego będą przekazywane dane osobowe oraz mapowanie procesów, w ramach których transfer będzie się dokonywał. Oczywiście jeżeli mówimy o transferze w ramach Europejskiego Obszaru Gospodarczego to będzie on zgodny z prawem każdorazowo po spełnieniu przesłanek legalizujących przetwarzanie danych osobowych w kraju macierzystym przetwarzania[333].

W sytuacji przekazywania danych do państwa trzeciego, proces ten może mieć miejsce, gdy Komisja Europejska w ramach decyzji stwierdzi, że to państwo zapewnia odpowiedni poziom ochrony danych osobowych. Przekazanie danych do miejsc objętych takimi decyzjami jest dopuszczalne bez konieczności podejmowania dodatkowych działań[334]. Na dzień 1 stycznia 2021 Komisja Europejska wydała takie decyzje wobec Andory, Argentyny, Wyspy Guernsey, Izraela, Japonii, Jersey, Kanady, Nowej Zelandii, Szwajcarii, Urugwajowi, Wyspy Man, Wysp Owczych czy USA (ale tylko w ramach tzw. Safe Harbour i Privacy Shield)[335].

TABELA 12 Lista państwa objętych decyzjami Komisji Europejskiej w sprawie transferu danych osobowych

Lp	Państwo	Decyzja KE	Uwagi
1.	Andora	Decyzja Komisji z dnia 19 października 2010 r. na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie odpowiedniej ochrony danych osobowych w Andorze	–
2.	Argentyna	Decyzja Komisji z dnia 30 czerwca 2003 r. na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady w sprawie właściwej ochrony danych osobowych w Argentynie	–
3.	Guernsey	Decyzja Komisji z dnia 21 listopada 2003 r. w sprawie właściwej ochrony danych osobowych w Guernsey	–
4.	Izrael	Decyzja Komisji z dnia 31 stycznia 2011 r. na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie odpowiedniej ochrony danych osobowych w Państwie Izrael w odniesieniu do zautomatyzowanego przetwarzania danych osobowych	Dotyczy wyłącznie danych przekazywanych z UE w związku z automatycznym przekazywaniem danych lub jeśli operacje przekazywania nie są zautomatyzowane, są one przedmiotem dalszego zautomatyzowanego przetwarzania w Izraelu.

[332] Szerzej zob. 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.

[333] Należy mieć na uwadze, że w ramach obowiązku informacyjnego (i w konsekwencji zakresu przedmiotowego zgody na przetwarzanie), podmiot którego dane są/będą przetwarzane powinien mieć wgląd do informacji na temat tego w ramach jakich obszarów jego dane będą poddawane transferom. Szerzej zob. *Adequacy decisions. How the EU determines if a non-EU country has an adequate level of data protection*, European Commission, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en#relatedlinks, [dostęp: 07.12.2020].

[334] Szerzej zob. 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.

[335] Szerzej zob. A. Michałowicz, *Nowe zasady transferu danych osobowych z Unii Europejskiej do Stanów Zjednoczonych w ramach Tarczy Prywatności*, Monitor Prawniczy 2016, nr 23, s. 1264–1271. Por. M. Rojszczak, *Skuteczność ochrony praw podmiotów danych wynikających z prawa UE w świetle umowy Tarcza Prywatności oraz prawodawstwa federalnego USA*, Transformacje Prawa Prywatnego 2018, nr 1.

Lp	Państwo	Decyzja KE	Uwagi
5.	Japonia	Decyzja wykonawcza Komisji (UE) 2019/419 z dnia 23 stycznia 2019 r. na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679, stwierdzająca odpowiedni stopień ochrony danych osobowych przez Japonię na mocy ustawy o ochronie informacji osobowych	Decyzja nie dotyczy wszystkich transferów danych. Zawiera wyłączenia dotyczące całych sektorów
6.	Jersey	Decyzja Komisji z dnia 8 maja 2008 r. na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie właściwej ochrony danych osobowych na Jersey	–
7.	Kanada	Decyzja Komisji z dnia 20 grudnia 2001 r. na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady w sprawie odpowiedniej ochrony danych osobowych zapewnionej w ustawie kanadyjskiej o ochronie informacji osobowych i dokumentów elektronicznych	Decyzja stwierdza, że Kanada jest krajem zapewniającym odpowiedni poziom ochrony danych osobowych przekazywanych ze Wspólnoty do odbiorców objętych przepisami ustawy kanadyjskiej o ochronie informacji osobowych i dokumentów elektronicznych.
8.	Nowa Zelandia	Decyzja wykonawcza Komisji z dnia 19 grudnia 2012 r. na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie odpowiedniej ochrony danych osobowych w Nowej Zelandii	–
9.	Szwajcaria	Decyzja Komisji z dnia 26 lipca 2000 r. na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady w sprawie właściwej ochrony danych osobowych w Szwajcarii	–
10.	Urugwaj	Decyzja wykonawcza Komisji z dnia 21 sierpnia 2012 r. na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie odpowiedniej ochrony danych osobowych przez Wschodnią Republikę Urugwaju w odniesieniu do zautomatyzowanego przetwarzania danych osobowych	Dotyczy wyłącznie zautomatyzowanego przetwarzania danych osobowych
11.	Wyspa Man	Decyzja Komisji z dnia 28 kwietnia 2004 r. w sprawie odpowiedniej ochrony danych osobowych na wyspie Man	–
12.	Wyspy Owcze	Decyzja Komisji z dnia 5 marca 2010 r. na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie właściwej ochrony na podstawie ustawy Wysp Owczych w sprawie ochrony danych osobowych	–
13.	USA (Safe Harbour)	Decyzja Komisji z dnia 26 lipca 2000 r. przyjęta na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie adekwatności ochrony przewidzianej przez zasady ochrony prywatności w ramach „bezpiecznej przystani" oraz przez odnoszące się do nich najczęściej zadawane pytania, wydane przez Departament Handlu USA	Nie działa wskutek orzeczenia TSUE, który stwierdził nieważność tej decyzji w wyroku z dnia 6.10.2015 r. Maximillian Schrems p-ko Data Protection Commissioner (Schrems I)
14.	USA (Privacy Shield)	Decyzja wykonawcza Komisji (UE) 2016/1250 z dnia 12 lipca 2016 r. przyjęta na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie adekwatności ochrony zapewnianej przez Tarczę Prywatności UE-USA	Decyzja 2016/1250 nie działa wskutek orzeczenia TSUE, który stwierdził nieważność tej decyzji w wyroku z dnia 16.07.2020 r. Data Protection Commissioner p-ko Facebook Ireland Ltd, Maximillian Schrems (Schrems II)
15.	USA (od 27.06. 2021)	Decyzja wykonawcza Komisji (UE) 2021/914 z dnia 4 czerwca 2021 r. w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 (Tekst mający znaczenie dla EOG	Decyzja 2021/914 obowiązuje do dnia 27 czerwca 2021r

Źródło: opracowanie własne na podstawie *Adequuacy decisions. How the EU determines if a non-EU country has an adequate level of data protection*, European Commission, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en#relatedlinks, [dostęp: 17.12.2020]

Sam fakt, że państwo do którego przekazywane są dane osobowe, znajduje się na liście Komisji Europejskiej nie jest jednak wystarczający. Szczegółowe warunki transferu danych określa bowiem sama decyzja dotycząca danego państwa. I tak nie we wszystkich przypadkach decyzje obejmują wszystkie przypadki transferu danych. Na przykład decyzja wydana względem Urugwaju, dotyczy wyłącznie zautomatyzowanego przetwarzania danych. Ponadto destynacja transferu danych względem którego obowiązuje decyzja, nie daję pewności, iż obejmuje ona całe państwo. Szczegółowa analiza treści decyzji może wskazywać, iż np. nie dotyczy ona całego terytorium, a jedynie podmioty zrzeszone w ramach dedykowanych organizacji. Takim przykładem są Stany Zjednoczone gdzie transfer objęty kolejnymi decyzjami KE dotyczył

do lipca 2020 roku (tj. do drugiego z wyroków TSUE w sprawie Schrems[336]) wyłącznie jednostek organizacyjnych działających w odpowiednich zrzeszeniach: początkowo w ramach Safe Harbour[337], a potem Privacy Shield[338].

Relacje informacyjne UE z USA w ogóle zostały w tym czasie poddane próbie, chociażby z uwagi na ujawnienie zjawiska zinstytucjonalizowanego podsłuchiwania najwyższych rangą urzędników unijnych przez amerykańską agencję wywiadowczą – National Security Agency (NSA)[339]. Na tę okoliczność powstało szereg dokumentów opisujących charakter transatlantyckiej wymiany danych[340], przy czym należy również mieć na uwadze zauważalną, od czasu ataków na World Trade Center, tendencję do poszerzania zakresu środków bezpieczeństwa kosztem prywatności obywateli[341] – i to zarówno w USA (*vide* Patriot Act[342]), jak i UE (*vide* dyrektywa retencyjna[343]).

Komisja Europejska, 4 czerwca 2021 roku[344], w odpowiedzi na wydany w lipcu 2020 roku wyrok Trybunału Sprawiedliwości Unii Europejskiej – Shrems II – unieważniający dotychczasową podstawę transferu jaką była decyzja Privacy Shield[345], przyjęła dwa zestawy nowych standardowych klauzul umownych. Są to:

1) decyzja wykonawcza Komisji (UE) 2021/914 z dnia 4 czerwca 2021 r. w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 (Tekst mający znaczenie dla EOG)[346],

---

[336] W wyroku z dnia 6.10.2015 r. w sprawie Maximillian Schrems p-ko Data Protection Commissioner (tzw. Schrems I) Trybunał Sprawiedliwości UE stwierdził nieważność decyzji Komisji z dnia 26 lipca 2000 r. ustalającej tzw. „bezpieczną przystań" (*Safe Harbour*), skutkiem czego Komisja wypracowała nową decyzję wykonawczą 2016/1250 z dnia 12 lipca 2016 r. wprowadzającą „tarczę prywatności" (*Privacy Shield*), która z kolei również została uznana za nieważną w wyroku z dnia 16.07.2020 r. w sprawie Data Protection Commissioner p-ko Facebook Ireland Ltd, Maximillian Schrems (Schrems II). Oznacza to, że po orzeczeniach TSUE, nawet organizacje z USA, zrzeszone w Safe Harbour czy Privacy Shield, będą traktowane tak samo jak państwa trzecie bez decyzji Komisji. Zob. *Przekazywanie danych do USA ponownie pod znakiem zapytania*, https://gdpr.pl/aktualnosci/przekazywanie-danych-do-usa-ponownie-pod-znakiem-zapytania, [dostęp: 07.12.2020]. Szerzej na temat prywatności w USA zob. A. Levin, M. Nicholson, *Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground*, University of Ottawa Law & Technology Journal 2005, nr. 2, s. 357–395.

[337] Wyrok TSUE z 6 października 2015 r. w sprawie Maximillian Schrems p-ko Data Protection Commissioner, tzw. Schrems I (C-362/14), https://sip.lex.pl/orzeczenia-i-pisma-urzedowe/orzeczenia-sadow/c-362–14-maximillian-schrems-v-data-protection-522014682, [dostęp: 07.12.2020].

[338] Wyrok TSUE z 16 lipca 2020 r. TSUE w sprawie Data Protection Commissioner przeciwko Facebook Ireland Ltd. i Maximilian Schrems, tzw. Schrems II (C-311/18), https://sip.lex.pl/orzeczenia-i-pisma-urzedowe/orzeczenia-sadow/c-311–18-przekazywanie-danych-obywateli-panstw-523123145, [dostęp: 07.12.2020].

[339] Zob. Rezolucja Parlamentu Europejskiego z 12.03.2014 r. w sprawie realizowanych przez NSA amerykańskich programów nadzoru, organów nadzoru w różnych państwach członkowskich oraz ich wpływu na prawa podstawowe obywateli UE oraz na współpracę transatlantycką w dziedzinie wymiaru sprawiedliwości i spraw wewnętrznych (2013/2188(INI), sygn. P7_TA(2014)0230. Na temat

[340] Zob. Rezolucja Parlamentu Europejskiego z 12.03.2014 r. w sprawie realizowanych przez NSA amerykańskich programów nadzoru, organów nadzoru w różnych państwach członkowskich oraz ich wpływu na prawa podstawowe obywateli UE oraz na współpracę transatlantycką w dziedzinie wymiaru sprawiedliwości i spraw wewnętrznych (2013/2188(INI), sygn. P7_TA(2014)0230. Por. Directorate General for Internal Policies Policy, The US legal system on data protection in the field of law enforcement. Safeguards, rights and remedies for EU citizens, Bruksela 2015.

[341] Szerzej na temat zagrożeń dla prywatności zob. A. Rogala-Lewicki, *Dane osobowe – zagrożenia wynikające z aktywności sektora państwowego w przestrzeni niejawnej*, Wiedza Prawnicza Nr 6/2013.

[342] Zob. European Parliament, Directorate General For Internal Policies, "The US surveillance programmes and their impact on EU citizens' fundamental rights", PE 474.405, Bruksela 2013. Szerzej zob. A. Rogala-Lewicki, *Security services after the terrorist attacks in the US and Europe. Patriot Act versus the Retention Directive, or the legitimization of abuses in the sphere of privacy in democratic states: a comparative study*, Myśl Ekonomiczna i Polityczna, Nr 3(50)/2015, ISSN: 2081–5913.

[343] Zob. European Parliament Directorate General for Internal Policies, National programmes for mass surveillance of personal data in EU Member States and their compatibility with EU law, Bruksela 2003; Directorate General for Internal Policies Policy, The US legal system on data protection in the field of law enforcement. Safeguards, rights and remedies for EU citizens, Bruksela 2015. Szerzej zob. A. Rogala-Lewicki, *European Intelligence Community – the unfulfilled pillar of the European Union*, Myśl Ekonomiczna i Polityczna, Nr 3(54)/2016, ISSN: 2081–5913. Por. A. Rogala-Lewicki, *Classified methods of collecting information on citizens. Comparative legal study of invigilation in Poland*, Studium Europy Środkowej i Wschodniej, Nr 14/2020, ISSN: 2353–8392.

[344] Projekty obu tych decyzji zostały przedstawione w listopadzie 2020 r. Do 10 grudnia 2020 r. Komisja Europejska przyjmowała opinie w ich sprawie. W styczniu 2021 r. wspólne opinie w tym zakresie przyjęły Europejska Rada Ochrony Danych (EROD) i Europejski Inspektor Ochrony Danych (EIOD). Nowe zestawy standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich zostały opublikowane w Dzienniku Urzędowym Unii Europejskiej w dniu 7 czerwca 2021 r. i weszły w życie 27 czerwca 2021 r. Zob. *Czym są standardowe klauzule umowne przyjęte przez KE?*, https://blog-daneosobowe.pl/czym-sa-standardowe-klauzule-umowne-przyjete-przez-ke-rodofaq/, [dostęp: 07.07.2021].

[345] Szerzej na temat Tarczy Prywatności zob. 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.

[346] Dz.Urz. UE L 199 z 7.6.2021, s. 31–61.

2) decyzja wykonawcza Komisji (UE) 2021/915 z dnia 4 czerwca 2021 r. w sprawie standardowych klauzul umownych między administratorami a podmiotami przetwarzającymi na podstawie art. 28 ust. 7 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 oraz art. 29 ust. 7 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 (Tekst mający znaczenie dla EOG)[347].

Nowe standardowe klauzule umowne (SKU) mają na celu zagwarantować bezpieczny transfer danych osobowych pomiędzy uczestnikami rynku, oraz zapewnić ich zgodność z wymogami RODO, w szczególności: do państw spoza EOG, tzw. państw trzecich pomiędzy administratorami oraz procesorami (decyzja 2021/914) oraz w ramach powierzeń danych (decyzja 2021/915). Odnoszą się zarówno do przepisów RODO (zawierają postanowienia wymagane na podstawie art. 28 ust. 3–4 RODO), jak i do przepisów rozporządzenia 2018/1725, które dotyczy przetwarzania danych przez organy unijne (klauzule zawierają postanowienia wymagane przez art. 29 ust. 3–4 rozporządzenia). Jednocześnie uwzględniają wspólną opinię Europejskiej Rady Ochrony Danych i Europejskiego Inspektora Ochrony Danych[348].

Podejście modułowe odróżnia nowe od dotychczas obowiązujących standardowych klauzul umownych, które przewidują odrębne SKU dla konkretnej sytuacji transferowej. Nowe SKU składają się bowiem z:

- klauzul ogólnych, które znajdują zastosowanie do wszystkich scenariuszy transferów (m.in. przepisy wstępne, przepisy dotyczące niezgodności i rozwiązania umowy);
- klauzul szczegółowych, które dzielą się na różne moduły w zależności od konkretnego scenariusza przekazywania danych do państwa trzeciego;
- załączników (zawierających listę stron, opis transferów, właściwy organ nadzorczy, środki techniczne i organizacyjne, w tym środki techniczne i organizacyjne zapewniające bezpieczeństwo danych, listę podprocesorów)[349].

W konsekwencji oprócz klauzul ogólnych administratorzy i podmioty przetwarzające powinni wybrać moduł mający zastosowanie do ich sytuacji, aby dostosować obowiązki spoczywające na nich na mocy klauzul do roli i obowiązków, jakie pełnią w związku z przetwarzaniem danych. Opracowane przez Komisję Europejską SKU nie są zatem uniwersalnym wzorem umowy, który można zastosować w każdym przypadku bez zmian czy uzupełnień. Ich wykorzystanie wymaga dostosowania do konkretnego przypadku powierzenia przetwarzania danych osobowych, przy czym korzystanie ze standardowych klauzul umownych opracowanych przez Komisję Europejską nie jest obowiązkowe[350].

[347] Dz.Urz. UE L 199 z 7.6.2021, s. 18–30.
[348] EDPB-EDPS Joint Opinion 2/2021 on standard contractual clauses for the transfer of personal data to third countries, European Data Protection Board, https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-22021-standard_en, [dostęp: 07.07.2021] oraz EDPB-EDPS Joint Opinion 1/2021 on standard contractual clauses between controllers and processors, European Data Protection Board, https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-12021-standard_en, [dostęp: 07.07.2021].
[349] I. Małobęcka-Szwast, *Nowe standardowe klauzule umowne*, https://www.traple.pl/2021/06/17/nowe-standardowe-klauzule-umowne/, [dostęp: 07.07.2021].
[350] Zob. *Czym są standardowe klauzule umowne przyjęte przez KE?*, https://blog-daneosobowe.pl/czym-sa-standardowe-klauzule-umowne-przyjete-przez-

Należy pamiętać, że standardowe klauzule umowne w zakresie umów powierzenia przetwarzania danych osobowych mogą być również opracowywane przez krajowe organy nadzorcze. Do dzisiaj takimi klauzulami, które zostały opublikowane na stronie Europejskiej Rady Ochrony Danych, są standardowe klauzule umowne duńskiego organu nadzorczego[351]. W Polsce, w styczniu 2019 roku, Prezes UODO ogłosił, że zamierza przyjąć zgodnie z art. 28 ust. 8 RODO standardowe klauzule umowne w zakresie umów powierzenia przetwarzania danych i rozpoczął konsultacje w ich sprawie[352].

W części dotyczącej przekazywania danych osobowych do państw trzecich, SKU są zestawione w konstrukcji modułowej, które w swoim stosowaniu uwzględniają cztery możliwości transferu[353]:

- pomiędzy administratorami z czego jeden z administratorów znajduje się w państwie trzecim (C2C),
- między administratorem a podmiotem przetwarzającym znajdującym się w państwie trzecim (C2P),
- pomiędzy podmiotami przetwarzającymi z czego jeden z podmiotów przetwarzających znajduje się w państwie trzecim (P2P),
- między podmiotem przetwarzającym a administratorem znajdującym się w państwie trzecim (P2C).

Podmioty, które dotychczas opierały przekazywanie danych do państw trzecich na wcześniejszych standardowych klauzulach dostały okres przejściowy na dostosowanie się do nowej regulacji. Mogą one w dalszym ciągu na ich podstawie przekazywać dane do państw trzecich przez okres łącznie 18 miesięcy:

- I etap – 3 miesiące od dnia przyjęcia nowych klauzul (po 27 czerwca br.) – w tym okresie możliwe jest zawieranie w nowych umowach wcześniejszych klauzul. Po tym okresie ma nastąpić uchylenie decyzji 2001/497/WE i 2010/87/UE zawierającej wcześniejsze klauzule umowne,
- II etap – 15 miesięcy od dnia uchylenia wcześniejszych klauzul czyli od zakończenia I etapu– w tym okresie, przy zawieraniu nowych umów, możliwe jest używanie jedynie nowych klauzul. W przypadku umów zawierających wcześniejsze klauzule umowne, zawartych przed

ke-rodofaq/, [dostęp: 07.07.2021].

[351] DK SA Standard Contractual Clauses for the purposes of compliance with art. 28 GDPR (January 2020), European Data Protection Board, https://edpb.europa.eu/our-work-tools/our-documents/decision-sa/dk-sa-standard-contractual-clauses-purposes-compliance-art_en, [dostęp: 07.07.2021]. Należy przy tym zauważyć, że Europejska Rada Ochrony Danych Osobowych wydała kilka opinii w sprawie projektu standardowych klauzul umownych przedłożonych przez krajowe organy nadzorcze (art. 28 ust. 8 RODO), w tym przez organ: duński – 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, słoweński – Opinion 17/2020 on the draft Standard Contractual Clauses submitted by the SI SA (Article 28(8) GDPR), European Data Protection Board, https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-172020-draft-standard-contractual-clauses_en, [dostęp: 07.07.2021], czy litewski – Opinion 18/2021 on the draft Standard Contractual Clauses submitted by the LT SA (Article 28(8) GDPR), European Data Protection Board, https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-182021-draft-standard-contractual-clauses_pl, [dostęp: 07.07.2021]. W ww. Opiniach Rada prezentowała stanowisko, iż przedłożone do zaopiniowania projekty SKU wymagają dalszych dostosowań, aby można je było uznać za standardowe klauzule umowne. Nadto przedstawiła kilka zaleceń, od których wdrożenia przez organ nadzorczy uzależniła wykorzystanie projektu standardowych klauzul umownych, zgodnie z art. 28 ust. 8 RODO bez konieczności ich późniejszego przyjęcia przez Komisję Unii Europejskiej.

[352] Termin zgłoszenia stanowisk upłynął 1 lutego 2019 roku. Zob. *Prezes UODO rozpoczyna konsultacje dotyczące umów powierzenia przetwarzania danych*, https://uodo.gov.pl/pl/138/650, [dostęp: 07.07.2021].

[353] *Transfer danych do państw trzecich zgodny z RODO*, https://uodo.gov.pl/pl/138/2085, [dostęp: 07.07.2021].

tym okresem, nie ma konieczności aktualizacji umów, jeżeli aktualizacja miałaby dotyczyć jedynie zmiany klauzul umownych. Konieczność aktualizacji klauzul umownych występuje jedynie w przypadku, gdy w trakcie II etapu nastąpi zmiana treści umowy. Wtedy konieczne jest również dokonanie aktualizacji standardowych klauzul umownych[354].

Standardowe klauzule umowne oparte o Dyrektywę 95/46/WE będą obowiązywać zatem maksymalnie do 27 grudnia 2022 roku. Oznacza to, że przeniesienie dotychczasowych transferów danych osobowych ze starych na nowe klauzule powinno nastąpić do tej daty.

Jeżeli transfer danych dotyczy terytorium spoza EOG, który jednocześnie nie jest objęty decyzją Komisji Europejskiej, legalizacja przekazywania danych, będzie wymagała podjęcia bardziej złożonych działań. Rozwiązania można podzielić na te:

- standardowe, które RODO nazywa przekazywaniem z zastrzeżeniem odpowiednich zabezpieczeń (opisane w art. 46 i 47 RODO),
- wyjątkowe, stosowane jedynie w ostateczności (te przypadki opisuje art. 49 RODO)[355].

W przypadku zastosowania rozwiązań standardowych rozporządzenie daje aż osiem różnych możliwości, które można dodatkowo podzielić, na te wywołujące skutki bez udziału organu nadzorczego (pkt 1–6 RODO), oraz te wymagające dla swej skuteczności zezwolenia organu nadzorczego (pkt 7 i 8 RODO).

TABELA 13 Charakterystyka rozwiązań standardowych w zakresie legalizacji transferu danych poza EOG

Lp.	Rozwiązanie	Charakterystyka rozwiązania
1.	Standardowe klauzule ochrony danych przyjęte przez Komisję	Standardowe klauzule ochrony są formą umowy między jednostką organizacją z państwa nadawcy, a organizacją odbierającą dane. W kontrakcie odbiorca zobowiązuje się do przestrzegania określonych zasad przetwarzania danych osobowych. Komisja Europejska przygotowała gotowe, znajdujące się w domenie publicznej oraz dostępne we wszystkich unijnych językach klauzule umowne. Dotychczas zostały wydane trzy decyzje zawierające zestawy tzw. standardowych klauzul umownych[356]: (1) decyzja 2001/479/WE Komisji z 15.06.2001 r. w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich[357], (2) decyzja 2004/915/WE Komisji z 27.12.2004 r. zmieniająca decyzję 2001/497/WE w zakresie wprowadzenia alternatywnego zestawu standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich[358], (3) decyzja 2010/87/UE Komisji z 05.02.2010 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[359]. Należy mieć na uwadze, że klauzule stanowią umowę w rozumienia prawa cywilnego ze wszystkimi konsekwencjami, w szczególności w zakresie swobody decyzyjnej podmiotu zewnętrznego do podpisania takich umów.

[354] K. Bodzak, *Nowe standardowe klauzule umowne Komisji Europejskiej*, https://rodoradar.pl/nowe-standardowe-klauzule-umowne-komisji-europejskiej/, [dostęp: 07.07.2021].

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

[356] Klauzule wprowadzone przed dwie pierwsze decyzje, mają zastosowanie do przekazywania danych pomiędzy administratorami danych (udostepnienie), natomiast klauzule wprowadzone na podstawie trzeciej decyzji, znajdują zastosowanie przy przekazywaniu danych podmiotowi przetwarzającemu dane osobowe na zlecenie (powierzenie). Treść klauzul odwołuje się nie do RODO, ale do dyrektywy 95/46/WR, którą RODO zastąpiło. Nie przeszkadza to jednak w ich stosowaniu, gdyż decyzje wydane przez Komisję na podstawie dyrektywy 95/46/WE w odniesieniu do standardowych klauzul umownych pozostają w mocy do czasu ich zmiany, zastąpienia lub uchylenia w razie potrzeby decyzją Komisji. Zob. *Przekazywanie danych osobowych do państw trzecich zgodnie z RODO… czyli jak?*, https://blog-daneosobowe.pl/przekazywanie-danych-osobowych-do-panstw-trzecich-zgodnie-z-rodo/, [dostęp: 10.12.2020].

[357] Decyzja 2001/479/WE Komisji z 15.06.2001 r. w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich, http://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32001D0497&from=en, [dostęp: 10.12.2021].

[358] Decyzja 2004/915/WE Komisji z 27.12.2004 r. zmieniająca decyzję 2001/497/WE w zakresie wprowadzenia alternatywnego zestawu standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:385:0074:0084:PL:PDF, [dostęp: 10.12.2021].

[359] Decyzja 2010/87/UE Komisji z 05.02.2010 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, http://eur-lex.europa.eu/

Lp.	Rozwiązanie	Charakterystyka rozwiązania
2.	Wiążące reguły korporacyjne	Wiążące reguły korporacyjne to przyjmowane wewnętrznie przez międzynarodowe koncerny standardy określonych obowiązków w celu jednolitego przestrzegania przez wszystkie podmioty zależne. W praktyce jest to narzędzie adresowane do międzynarodowych grup kapitałowych, które mogą opracować i wdrożyć jednolitą politykę ochrony danych osobowych dla wszystkich podmiotów z grupy. Przy czym taka polityka musi zostać zatwierdzona przez organ nadzorczy (np. polski UODO) zgodnie z mechanizmem spójności przewidzianym w RODO. Jednocześnie nie ma gotowych standardów, jak w przypadku klauzul przyjętych przez Komisję.
3.	Standardowe klauzule ochrony danych przyjęte przez organ nadzorczy i zatwierdzone przez Komisję	Rozwiązanie analogiczne do gotowych standardów Komisji Europejskiej, tylko opracowywane przez krajowe urzędy nadzoru i następnie zatwierdzane przez Komisję Europejską. Polski Urząd Ochrony Danych Osobowych, jak dotąd nie przyjął żadnej wersji standardowych klauzul ochrony danych.
4.	Zatwierdzony kodeks postępowania	Mechanizm pozwala organom nadzoru zatwierdzić kodeks postępowania zgodnie z art. 40 RODO, który zawiera wiążące i egzekwowalne zobowiązania administratora lub podmiotu przetwarzającego w państwie trzecim do stosowania odpowiednich zabezpieczeń. Kodeks ten później musi przyjąć organizacja w państwie trzecim. Jak dotąd trwają prace nad 30 kodeksami postępowania w Polsce. Europejska Rada Ochrony Danych ma zaopiniować polskie wymogi.
5.	Zatwierdzony mechanizm certyfikacji	Mechanizm pozwala organom nadzoru zatwierdzić mechanizm certyfikacji. W praktyce wciąż brak zatwierdzonych mechanizmów certyfikacji.
6.	Klauzule umowne pomiędzy podmiotami transferującymi dane	Narzędzie pozwala przygotować własne klauzule umowne, niemniej konieczny jest finalny akcept organu nadzorczego.
7.	Prawnie wiążący i egzekwowalny instrument między organami i podmiotami publicznymi	Rozwiązanie dostępne tylko dla podmiotów publicznych bez konieczności uzyskania zgody Prezesa UODO. Przesłanka ta obejmuje swym zakresem szeroko rozumiane umowy międzynarodowe oraz inne uzgodnienia administracyjne, jeżeli w świetle prawa międzynarodowego publicznego oraz prawa krajowego ich stron będą one miały wiążący prawnie charakter.
8.	Uzgodnienia administracyjne między organami lub podmiotami publicznymi	Rozwiązanie to odnosi się jedynie do podmiotów publicznych. W tym wypadku również wymaga się samodzielnego przygotowania treści uzgodnienia oraz dodatkowo pozyskania zezwolenia organu nadzorczego. Transfer danych jest także możliwy za zgodą Prezesa UODO na podstawie uzgodnień administracyjnych między organami lub podmiotami publicznymi, w których przewidziane będą egzekwowalne i skuteczne prawa osób, których dane dotyczą.

Źródło: opracowanie własne na podstawie: *Transfer danych osobowych poza Europejski Obszar Gospodarczy*, https://odoserwis.pl/a/1243/transfer-danych-osobowych-poza-europejski-obszar-gospodarczy-eog, [dostęp: 09.12.2021]

W praktyce zdecydowanie najczęściej stosowanym rozwiązaniem są standardowe klauzule ochrony danych przyjęte przez Komisję Europejską[360]. Do czasu wydania przez Trybunał Sprawiedliwości Unii Europejskiej 16 lipca 2020 roku orzeczenia w sprawie Schrems II, rozwiązania z art. 46 rozporządzenia były względnie proste w stosowaniu. Znaczące zmiany w zakresie transferu danych do państw trzecich, wprowadzone w/w orzeczeniem, odnoszą się do trzech zasadniczych kwestii:

1) uchylenia tzw. Tarczy Prywatności (*Privacy Shield*), na podstawie której dokonywano transferu danych osobowych do Stanów Zjednoczonych;
2) utrzymania w mocy 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 (decyzja Komisji Europejskiej z 5.2.2010 r. notyfikowana jako dokument nr C (2010) 593);
3) konieczności podejmowania przez administratorów danych dodatkowych środków, w zależności od poziomu ochronnych danych w danym państwie trzecim[361].

Po pierwsze TSUE zakwestionował zasady i istotę decyzji Komisji legalizującej transfer do tych podmiotów z USA, które znajdowały się w programie Privacy Shield[362]. TSUE w swoim

LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:PL:PDF, [dostęp: 10.12.2021].

[360] Przygotowany przez Komisję draft umowy, uzupełnia się we wskazanych miejscach, podpisuje i transfer jest zalegalizowany. Kontrahent wdraża (a przynajmniej w to wierzymy) zasady, o których mowa w standardowych klauzulach i gotowe! Pamiętaj jedynie o tym, że draft przygotowany przez Komisję nie podlega negocjacjom. Chyba, że w kierunku zwiększenia poziomu ochrony danych osobowych. Zob. *Przekazywanie danych osobowych do państw trzecich zgodnie z RODO… czyli jak?*, https://blog-daneosobowe.pl/przekazywanie-danych-osobowych-do-panstw-trzecich-zgodnie-z-rodo/, [dostęp: 10.12.2020].

[361] Zob. C. Kuner, *Reality and Illusion in EU Data Transfer Regulation Post Schrems*, University of Cambridge Faculty of Law Research Paper 2016, nr 14.

[362] Po wyroku Trybunału Sprawiedliwości UE z 6 października 2015 r. w sprawie Maksymiliana Schremsa, stwierdzającym nieskuteczność ochrony danych

orzeczeniu, dokonał oceny dopuszczalności przekazywania danych osobowych do Stanów Zjednoczonych, na podstawie standardowych klauzul umownych przyjętych przez Komisję. Doszło do delegalizacji dokonywania transferów na jej podstawie. Wyrok dotyczył decyzji KE nr 2010/87/UE, regulującej transfer danych, w ramach którego eksporter danych jest administratorem, a importer danych z państwa trzeciego jest podmiotem przetwarzającym (powierzenie). Zawarte tam wskazówki znajdują zastosowanie również w przypadku pozostałych dwóch zestawów klauzul, a więc klauzul administrator–administrator.

Sędziowie orzekli, że samo posługiwanie się standardowymi klauzulami ochrony danych zatwierdzonymi przez Komisję Europejską nie we wszystkich przypadkach czyni transfer danych do państwa trzeciego dopuszczalnym. Wskazano, że bardzo często podmioty podpisały standardowe klauzule w praktyce nigdy nie mając zamiaru wdrażać postanowień w nich zawartych.

Podmioty zaangażowane w transfer mają obowiązek dokonania uprzedniej analizy ustawodawstwa wewnętrznego importera danych, w szczególności pod kątem zasad dostępu do przekazywanych danych podmiotów publicznych. Gdy analiza ochrony danych w państwie trzecim da wynik negatywny, wówczas należy zadbać o dodatkowe środki ochrony danych w państwie trzecim[363]. Trybunał w ten sposób dokonał wykładni art. 46 ust. 1 rozporządzenia, przy czym nie sprecyzował jakie „dodatkowe środki" mają podejmować podmioty dokonujące przekazania danych poza obszar unijny ([364]:

- Rekomendacje 01/2020 w sprawie środków, które uzupełniają narzędzia transferu w celu zapewnienia zgodność z unijnym poziomem ochrony danych osobowych,
- Rekomendacje 2/2020 w zakresie europejskich gwarancji podstawowych dotyczących środków nadzoru (EEG)[365].

Wytyczne zostały przyjęte w celu pomocy eksporterom danych w złożonym procesie oceny poziomu ochrony danych w państwie trzecim i identyfikacji dodatkowych środków

osobowych w relacjach z USA realizowanej na postawie tzw. Decyzji KE Safe Harbour, przyjęto nową decyzję, tzw. Privacy Shield (Tarczy Prywatności), przewidującą zwiększenie kontroli, w tym m.in. obowiązek prowadzenia przez Departament Handlu Stanów Zjednoczonych listy firm, które zapewniają odpowiedni standard ochrony danych osobowych. Firmy te miały być regularnie weryfikowane pod kątem zapewnienia bezpieczeństwa przetwarzanym danym, zapewnienie kontroli sądowej nad dostępem do danych przez służby bezpieczeństwa USA, powołanie po stronie amerykańskiej Rzecznika przy Departamencie Stanu, który miał być odpowiednikiem europejskich organów nadzorczych w zakresie ochrony danych osobowych, zwiększenie uprawnień osób, których dane dotyczą oraz dokonywania przez Komisję Europejską i Departament Handlu USA regularnych przeglądów funkcjonowania zasad określonych w Tarczy Prywatności. W rzeczywistości zarejestrowanie się przez firmę z USA w Privacy Shield było bardzo proste – wystarczyło oświadczenie, w którym firma zobowiązywała się wdrożyć u siebie procedury ochrony danych osobowych zbliżone do tych przewidzianych w RODO. W praktyce zabrakło możliwości skutecznej egzekucji stosowania tych zasad. W państwach EOG na ich straży ochrony danych osobowych stoi organ europejski oraz lokalne organy nadzorcze z bogatą i wieloletnią praktyką, podczas gdy w Stanach Zjednoczonych nie ma żadnego wyspecjalizowanego organu. Zob. M. Szczotkowska, *Regulacje prawne transferu danych osobowych obywateli UE do USA – prawnoporównawcza analiza programu Safe Harbour i programu Privacy Shield*, Folia Iuridica Universitatis Wratislaviensis 2016, nr. 5 (1), s. 85–100. Por. Wystąpienie EROD przed TSUE w sprawie C-311/18 (Facebook Ireland i Schrems), przyjęte 9 lipca 2019 r., Europejska Rada Ochrony Danych.

[363] Zob. B. Mucha, *Data mining a współczesny kształt prawa do prywatności w Stanach Zjednoczonych Ameryki* [w:] *Efektywność europejskiego systemu ochrony praw człowieka. Ewolucja i uwarunkowania europejskiego systemu ochrony praw człowieka*, red. Jaskiernia J., Toruń 2012.

[364] Chodzi o fragment, w którym stwierdza się, że gdy zapewnią odpowiednie zabezpieczenia, i pod warunkiem, że obowiązują egzekwowalne prawa osób, których dane dotyczą, i skuteczne środki ochrony prawnej" co skutkuje koniecznością każdorazowego doprecyzowania do konkretnego przypadku standardowych klauzul umownych. Zob. *Wytyczne EROD w sprawie przesyłania danych do państw trzecich*, https://gdpr.pl/wytyczne-erod-w-sprawie-przesylania-danych-do-panstw-trzecich, [dostęp: 10.12.2020].

[365] Zob. (a) Zalecenia 2/2020 w sprawie niezbędnych gwarancji europejskich dla środków nadzoru, przyjęte 10 listopada 2020 r., Europejska Rada Ochrony Danych, (b) 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.

niezbędnych do zapewnienia odpowiedniego poziomu ochrony przekazywanych danych[366]. EROD określiła sześć podstawowych kroków do podjęcia:

- Krok 1: identyfikacja wszystkich dokonywanych transferów do państw trzecich[367];
- Krok 2: weryfikacja podstawy przekazywania danych[368];
- Krok 3: ocena systemu prawnego (legislacji i praktyki) w zakresie danych osobowych w danym państwie trzecim (ocena taka winna być udokumentowana)[369];
- Krok 4: identyfikacja i przyjęcie dodatkowych środków technicznych wzmacniających poziom ochrony przekazywanych danych, tak by osiągnął unijny standard np. poprzez szyfrowanie czy pseudonimizację (ocena taka winna być udokumentowana)[370];
- Krok 5: podjęcie kroków formalnych i proceduralnych w celu przyjęcia dodatkowego środka ochrony danych (np. w formie dodatkowych klauzul umownych)[371];
- Krok 6: monitorowanie sytuacji w państwach trzecich (w tym zmian w prawie) oraz weryfikowanie przyjętych wcześniej środków ochrony danych.

Wszystkie powyższe kroki powinny być podejmowane przy uwzględnieniu ogólnych zasad ochrony danych, przede wszystkim zasady zgodności z prawem, adekwatności[372] i rozliczalności[373]. Sposób oceny, zastosowane dodatkowe środki, jak również sposób ich wyboru i wdrożenia powinny zostać odpowiednio udokumentowane. Z wytycznych wynika, że organy nadzorcze powinny zwracać szczególną uwagę na działania podejmowane przez eksporterów danych w celu zapewnienia, że przekazywane przez nich dane objęte są odpowiednim poziomem ochrony. W przypadkach stwierdzenia, iż taki poziom ochrony nie został zapewniony, mają obowiązek wstrzymać lub zakazać przekazywania danych[374].

Jeżeli standardowe rozwiązania, opisane w art. 46 i 47 RODO, nie są możliwe do spełnienia, przy czym transfer danych poza terytorium EOG jest nadal konieczny, można odwołać się do rozwiązań wyjątkowych przewidzianych w art. 49 rozporządzenia. Przepis dopuszcza

[366] *EDPB Releases Guidance for EU-US Data Transfers*, https://digit.fyi/edpb-releases-guidance-for-eu-us-data-transfers/, [dostęp: 10.12.2020].

[367] W praktyce sprowadza się to przede wszystkim do zweryfikowania prowadzonych rejestrów czynności przetwarzania, kategorii czynności przetwarzania oraz obowiązków informacyjnych realizowanych względem podmiotów danych.

[368] Mogą to być decyzje stwierdzające odpowiedni poziom ochrony danych przyjmowane przez Komisję Europejską w trybie art. 45 RODO, przekazywanie danych z zastrzeżeniem odpowiednich zabezpieczeń, o których mowa w art. 46 RODO lub odstępstwa wymienione w przepisie art. 49 RODO.

[369] W załączniku do wytycznych wymieniono przykładowe źródła informacji, w tym m.in. orzecznictwo krajowe lub decyzje podjęte przez niezależne organy sądowe lub administracyjne właściwe w zakresie prywatności i ochrony danych w państwach trzecich, raporty instytucji akademickich, organizacji pozarządowych, stowarzyszeń branżowych.

[370] W załączniku do wytycznych wymienione zostały przykłady dodatkowych środków ochrony danych, które mogą być stosowane przez podmioty przekazujące dane do państw trzecich, a wśród nich: (a) środki techniczne, np. anonimizacja, szyfrowanie danych, (b) środki organizacyjne, jak np. procedury wewnętrzne, (c) środki umowne, tj. uwzględnianie w umowach dotyczących transferu danych odpowiednich klauzul ochronnych.

[371] Możliwe jest w tym zakresie zastosowanie standardowych klauzul ochrony danych przyjętych przez Komisję (art. 46 ust. 2 lit. c i d RODO), wiążących reguł korporacyjnych (art. 46 ust. 2 lit. b RODO), jak również klauzul umownych między administratorem lub podmiotem przetwarzającym a administratorem, podmiotem przetwarzającym lub odbiorcą danych osobowych w państwie trzecim lub organizacji międzynarodowej pod warunkiem uzyskania zezwolenia właściwego organu nadzorczego (art. 46 ust. 3 lit. a RODO). Zob. Transfer danych osobowych do państw trzecich: Stosowanie art. 26 ust. 2 dyrektywy o ochronie danych do wiążących reguł korporacyjnych dla międzynarodowych transferów danych, WP 74, Grupa robocza art. 29. Por. 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.

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

[373] *RODO: Przekazywanie danych osobowych do państw trzecich. Czyli co każdy administrator powinien sprawdzić przed dokonaniem transferu*, https://www2.deloitte.com/pl/pl/pages/doradztwo-prawne/articles/ochrona-danych-osobowych/newsletter-rodo0/RODO-przekazywanie-danych-osobowych-do-panstw-trzecich.html, [dostęp: 11.12.2020].

[374] *Projekt wytycznych Europejskiej Rady Ochrony Danych osobowych w sprawie transferu danych poza UE został opublikowany*, https://legalis.pl/projekt-wytycznych-europejskiej-rady-ochrony-danych-osobowych-w-sprawie-transferu-danych-poza-ue-zostal-opublikowany/, [dostęp: 11.12.2020].

przekazywanie danych do państwa trzeciego, które nie zapewnia odpowiedniego poziomu ochrony lub gdy nie zapewniono odpowiednich zabezpieczeń jak standardowe klauzule umowne czy wiążące reguły korporacyjne, w następujących sytuacjach:

1) osoba, której dane dotyczą, poinformowana o ryzyku, z którym – ze względu na brak decyzji stwierdzającej odpowiedni stopień ochrony oraz na brak odpowiednich zabezpieczeń – może się dla niej wiązać proponowane przekazanie danych, jednoznacznie wyraziła zgodę, przy czym musiała ona: (a) być wyraźna, (b) dotyczyć konkretnie danego jednorazowego/wielokrotnego przekazania danych, oraz (c) być świadoma, w szczególności osoba udzielająca zgody musi być zdawać sobie sprawę z ewentualnego ryzyka, z którym może się wiązać przekazanie[375],
2) przekazanie jest 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[376],
3) przekazanie jest niezbędne do zawarcia lub wykonania umowy zawartej w interesie osoby, których dane dotyczą, między administratorem a osobą fizyczną lub prawną[377],
4) przekazanie jest niezbędne ze względu na ważne względy interesu publicznego[378],
5) przekazanie jest niezbędne do ustalenia, dochodzenia lub ochrony roszczeń[379],
6) przekazanie jest niezbędne do ochrony żywotnych interesów osoby, których dane dotyczą, lub innych osób, jeżeli są fizycznie/prawnie niezdolna/i do wyrażenia zgody[380],
7) przekazanie danych następuje z publicznego rejestru[381],
8) przekazanie jest niezbędne ze względu na ważne prawnie uzasadnione interesy administratora i zostały spełnione dodatkowe wymogi[382].

Należy mieć na uwadze, że zastosowanie art. 49 RODO powinno mieć miejsce jedynie w wyjątkowych przypadkach i *de facto* adresowane jest do niewielkich jednostek organizacyjnych przetwarzających dane poza obszar EOG incydentalnie i w niewielkim zakresie. Na ten temat stanowisko zajęła Grupa Robocza art. 29 w relewantnych Wytycznych[383] negatywnie oceniając

[375] Wyraźna zgoda osoby, której dane dotyczą (art. 49 ust. 1 lit. a RODO). W przypadkach przekazywania danych osobowych pracowników, zgoda będzie ryzykownym rozwiązaniem (trudność w wykazaniu jej dobrowolności). Szerzej zob. C. Martysz, *Prawa osoby w świetle ustawy o ochronie danych osobowych* [w:] *Prawne i finansowe aspekty funkcjonowania samorządu terytorialnego*, Tom 1: Prawo samorządowe i administracyjne, red. S. Dolaty, Opole 2000.

[376] Art. 49 ust. 1 lit. b RODO. Dotyczy wykonania umów między osobą, której dane dotyczą a administratorem.

[377] Art. 49 ust. 1 lit. c RODO. Dotyczy umów zawartych pomiędzy podmiotem danych a administratorem.

[378] Art. 49 ust. 1 lit. d RODO. Przekazywanie danych osobowych celem przeciwdziałania terroryzmowi, celem zwalczania procederu prania brudnych pieniędzy, przekazywanie danych pomiędzy urzędami celnymi, podatkowymi czy dla celów ubezpieczeń społecznych, itp. Szerzej zob. np. Oświadczenie w sprawie ochrony danych osobowych przetwarzanych w związku z zapobieganiem praniu pieniędzy i finansowaniu terroryzmu, przyjęte 15 grudnia 2020 r., Europejska Rada Ochrony Danych.

[379] Art. 49 ust. 1 lit. e RODO. Należy pamiętać, że przesłanka ta dotyczy wyłącznie roszczeń lub wykazania ich bezzasadności przez administratora przekazującego dane.

[380] Art. 49 ust. 1 lit. f RODO. Przesłanka możliwa do zastosowania w sytuacjach kiedy osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody (ratowanie życia lub zdrowia osoby, której dane dotyczą).

[381] Art. 49 ust. 1 lit. g RODO W przypadku rejestrów publicznych, skoro dane osobowe i tak są dostępne dla nieograniczonej liczby osób, nie istnieje powód dla ograniczania możliwości przekazywania tych danych do państw trzecich.

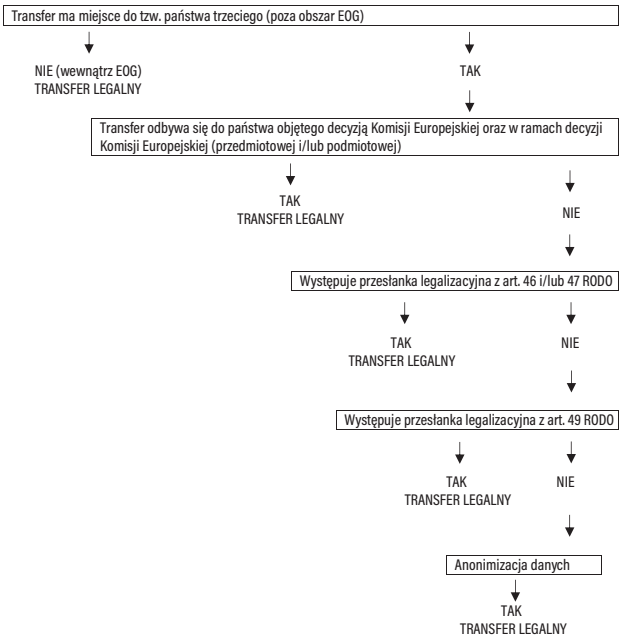
[382] Art. 49 ust. 1 akapit drugi RODO. Wyjątek od wyjątków odnosi się do sytuacji, która może mieć miejsce wtedy, kiedy nie można zalegalizować transferu danych ani na mocy art. 45 ani 46 RODO ani na podstawie art. 49 ust. 1 akapit pierwszy RODO. Dodatkowe wymogi to m.in.: przekazanie nie może być powtarzalne, może dotyczyć tylko ograniczonej liczby osób, musi być niezbędne ze względu na ważne prawnie uzasadnione interesy realizowane przez administratora, który ocenił wszystkie okoliczności przekazania danych i na podstawie tej oceny zapewnił odpowiednie zabezpieczenia. O takim transferze należy dodatkowo poinformować organ nadzorczy.

[383] Wytyczne 2/2018 w sprawie wyjątków określonych w art. 49 rozporządzenia 2016/679, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_pl, [dostęp: 12.12.2020].

praktykę dużych korporacji oraz jednostek publicznych, które mając ku temu prawne, finansowe i organizacyjne możliwości, nie korzystały z takich instrumentów, jak standardowe kontrakty oparte na rozwiązaniach gwarantujących wysoki poziom bezpieczeństwa, czy w przypadku korporacji dodatkowo wiążących reguł korporacyjnych[384]. Oznacza to, że duże podmioty realnie nie powinny korzystać z art. 49 RODO, a zatem muszą raz jeszcze rozważyć skorzystanie z standardowych kryteriów. Przy czym przesłanki legalizacyjne z art. 49 mogą być w drodze wyjątku pomocne do czasu legalizacji przetwarzania z podstaw opisanych w art. 46 i 47 rozporządzenia[385].

Ostatnią deską ratunku, na wypadek braku możliwości skorzystania zarówno z przesłanek standardowych, jak i wyjątkowych, jest anonimizacja danych osobowych podlegających transferowi co skutkuje *de facto* rezygnacją z transferu informacji o charakterze danych osobowych. Należy mieć na uwadze jednak, że anonimizacja jest kosztowna, oraz często niemożliwa do zastosowania w praktyce. Niemożność skorzystania z jakiejkolwiek przesłanki legalizacyjnej, jak również z anonimizacji skutkuje brakiem możliwości przekazywania danych osobowych w ogóle.

RYSUNEK 19 Drzewo decyzyjne w ramach transferu danych osobowych za granicę



Źródło: opracowanie własne na podstawie: *Transfer danych osobowych*, https://blog-daneosobowe.pl/wp-content/uploads/2020/12/lex_infografika_transfer_panstwo_trzecie.png, [dostęp: 12.12.2020]

[384] Zob. Dokument roboczy ustanawiający procedurę współpracy w celu zatwierdzenia „wiążących reguł korporacyjnych" dla administratorów i podmiotów przetwarzających zgodnie z RODO, przyjęty 11 kwietnia 2018r., 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

[385] Szerzej zob. *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, red. Sakowska-Baryła, Warszawa 2018.

Podmiot planujący przekazanie danych osobowych do państw trzecich powinien zatem przeanalizować, który z odpowiednich scenariuszy może znaleźć zastosowanie w jego sytuacji. Wybór będzie zależał od tego, czy przekazanie danych odbywa się w ramach grupy przedsiębiorstw, czy odbiorca danych legitymuje się zatwierdzonym certyfikatem[386], czy chce podpisać umowę zawierającą odpowiednie klauzule ochrony danych bądź przyjąć właściwy kodeks postępowania.

Podsumowując, zgodnie z wytycznymi EROD, administratorzy są zobowiązani do sprawdzenia w każdym przypadku, czy dane, które są transferowane poza UE są adekwatne, stosowne i ograniczone do tego, co jest konieczne w świetle celów w jakich są one przekazywane do państw trzecich. Oprócz wdrożenia odpowiednich zabezpieczeń należy zapewnić, iż transfer danych nie wpłynie negatywnie na możliwość skutecznego egzekwowania praw podmiotów danych. Kluczowym zagadnieniem jest tutaj tzw. rozliczalność. EROD w opublikowanych wytycznych podkreślił doniosłość zasady rozliczalności, która wymaga stałego nadzoru nad poziomem ochrony danych osobowych. Administratorzy – zdaniem EROD – powinni po pierwsze dokonywać oceny przepisów w zakresie ochrony danych osobowych, obowiązujących w państwie trzecim, po drugie przeprowadzać cykliczne oceny poziomu ochrony danych osobowych przekazywanych poza EOG.

Wzmocnienie współpracy pomiędzy organami nadzoru państw członkowskich oraz ustanowienie organu z uprawnieniami do wydawania wytycznych i wiążących decyzji

Rozporządzenie wprowadziło ustrukturyzowany model współpracy pomiędzy organami nadzoru ochrony danych osobowych państw członkowskich UE[387]. Zgodnie z mechanizmem spójności organy nadzorcze współpracują ze sobą, a w stosownym przypadku także z Komisją[388], stosując wszelkie mechanizm prawne przewidziane w RODO. Przepis art. 61 precyzuje narzędzia wzajemnej pomocy. I tak zgodnie z normą organy nadzorcze przekazują sobie stosowne informacje i świadczą sobie wzajemną pomoc w celu spójnego wdrażania i stosowania rozporządzenia oraz wprowadzają środki na rzecz skutecznej wzajemnej współpracy. Wzajemna pomoc obejmuje w szczególności wnioski o udzielenie informacji oraz środki nadzorcze, takie jak wnioski o udzielenie uprzednich zezwoleń i przeprowadzenie uprzednich konsultacji oraz o przeprowadzenie kontroli i postępowań wyjaśniających. Każdy organ nadzorczy podejmuje wszelkie odpowiednie środki, by odpowiedzi na wniosek innego organu nadzorczego udzielić bez zbędnej zwłoki i nie później niż w terminie miesiąca od otrzymania wniosku. Środki takie mogą obejmować w szczególności przekazanie stosownych informacji o przebiegu postępowania[389].

[386] Szerzej na temat certyfikacji zob. T. Osiej, *Charakter prawny nowych mechanizmów certyfikacji w zakresie ochrony danych osobowych*, Informacja w administracji publicznej 2017, nr 2.

[387] Szerzej zob. EDPB Statement: EDPB cooperation on the elaboration of guidelines, przyjęte 16 grudnia 2021r., Europejska Rada Ochrony Danych

[388] Komisja może w drodze aktów wykonawczych określić może formułę i procedurę wzajemnej pomocy oraz zasady wymiany informacji drogą elektroniczną między organami nadzorczymi oraz między organami nadzorczymi a Europejską Radą Ochrony Danych, w szczególności standardowy format. Jednocześnie przepis art. 60 ust. 12 wprost wprowadza dany standard stanowiąc, iż w ramach współpracy wiodący organ nadzorczy i inne organy nadzorcze, których sprawa dotyczy, dostarczają sobie nawzajem informacji drogą elektroniczną w standardowym formacie. Zob. art. 67 oraz art. 60 ust. 12 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 (Dz. Urz. UE L 119 z dn. 4.05.2016, s. 1–88).

[389] Art. 61 ust. 1–2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych

Organy nadzory mogą bezpośrednio pomiędzy sobą zwrócić się z tzw. wnioskiem o pomoc. Wezwany organ nadzorczy nie może odmówić wykonania wniosku, chyba że: (a) nie jest organem właściwym w przedmiocie wniosku lub środków, o których wykonanie wystąpiono lub (b) wykonanie wniosku stanowiłoby naruszenie rozporządzenia, prawa Unii lub prawa państwa członkowskiego, któremu podlega wezwany organ nadzorczy. Wezwany organ nadzorczy informuje wzywający organ nadzorczy, od którego wniosek pochodzi, o rezultatach lub w stosownym przypadku o postępach lub środkach zastosowanych w związku z tym wnioskiem[390].

Kolejnym – obok wniosku o pomoc – instrumentem materializowania współpracy organów nadzoru są tzw. wspólne operacje organów nadzorczych. Na mocy art. 62 rozporządzenia organy nadzorcze mogą prowadzić wspólne postępowania i wspólne działania egzekucyjne. Dotyczy to sytuacji gdy administrator lub podmiot przetwarzający posiadają jednostki organizacyjne w kilku państwach członkowskich lub jeżeli operacje przetwarzania mogą istotnie wpłynąć na znaczną liczbę osób, których dane dotyczą, w więcej niż jednym państwie członkowskim. Organ nadzorczy każdego z tych państw członkowskich ma prawo uczestniczyć we wspólnych operacjach.

Procedura wygląda następująco. Właściwy wiodący organ nadzorczy zaprasza organ nadzorczy każdego z relewantnych państw członkowskich do uczestnictwa w danych wspólnych operacjach i niezwłocznie odpowiada na wniosek organu nadzorczego dotyczący uczestnictwa. Organ nadzorczy może zgodnie z prawem państwa członkowskiego i za zgodą organu nadzorczego oddelegowującego pracownika przyznać uprawnienia, w tym uprawnienia do prowadzenia postępowań wyjaśniających, członkom lub personelowi organu nadzorczego oddelegowującego pracownika uczestniczącym we wspólnych operacjach lub – jeżeli zezwala na to prawo państwa członkowskiego przyjmującego organu nadzorczego – zezwolić członkom lub personelowi organu nadzorczego oddelegowującego pracownika na wykonywanie ich własnych uprawnień w zakresie prowadzenia postępowań wyjaśniających zgodnie z prawem państwa członkowskiego organu nadzorczego oddelegowującego pracownika. Uprawnienia takie mogą być wykonywane wyłącznie pod kierownictwem i w obecności członków lub personelu przyjmującego organu nadzorczego. Członkowie lub personel organu nadzorczego oddelegowującego pracownika podlegają prawu państwa członkowskiego przyjmującego organu nadzorczego. Jeżeli personel organu nadzorczego oddelegowującego pracownika działa w innym państwie członkowskim, państwo członkowskie przyjmującego organu nadzorczego ponosi odpowiedzialność za czynności tego personelu, w tym odpowiedzialność

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).

[390] Wezwane organy nadzorcze przekazują informacje żądane przez inne organy nadzorcze zasadniczo drogą elektroniczną w standardowym formacie. Wezwane organy nadzorcze nie pobierają opłat za działania podejmowane w związku z wnioskiem o wzajemną pomoc. Organy nadzorcze mogą uzgodnić zasady dokonywania wzajemnego zwrotu konkretnych wydatków poniesionych w wyniku świadczenia wzajemnej pomocy w wyjątkowych okolicznościach. Jeżeli organ nadzorczy nie dostarczy informacji zgodnie z wnioskiem w terminie miesiąca od otrzymania wniosku innego organu nadzorczego, wzywający organ nadzorczy może zastosować środek tymczasowy na terytorium swojego państwa członkowskiego. W takiej sytuacji uznaje się, że zgodnie z art. 66 ust. 1 zachodzi pilna potrzeba działania i że zgodnie z art. 66 ust. 2 wymagana jest pilna wiążąca decyzja Europejskiej Rady Ochrony Danych. Zob. art. 61 ust. 3–9 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 (Dz. Urz. UE L 119 z dn. 4.05.2016, s. 1–88).

prawną za wszelkie szkody wyrządzone przez ten personel w trakcie operacji[391], zgodnie z prawem państwa członkowskiego, na którego terytorium ten personel działa. Jeżeli planowana jest wspólna operacja, a organ nadzorczy nie wywiąże się w terminie miesiąca ze swojego obowiązku określonego, pozostałe organy nadzorcze mogą przyjąć środek tymczasowy na terytorium swojego państwa członkowskiego. W takiej sytuacji uznaje się, że zachodzi pilna potrzeba działania i wymagana jest pilna opinia lub pilna wiążąca decyzja Europejskiej Rady Ochrony Danych (na mocy art. 66 ust. 1 i 2)[392].

Rozporządzenie reguluje również formę współpracy w sytuacji prowadzonego postępowania przed organem wiodącym[393] oraz innymi organami nadzorczymi, których sprawa dotyczy, w szczególności organy zostały zobowiązane do wymieniania się wszelkimi stosownymi informacjami. Zgodnie z art. 60 RODO wiodący organ nadzorczy może w dowolnym momencie zwrócić się do innych organów nadzorczych, których sprawa dotyczy, o wzajemną pomoc (na mocy art. 61) i może prowadzić wspólne operacje (na mocy art. 62), w szczególności w celu przeprowadzenia postępowania lub monitorowania wdrażania środka dotyczącego administratora lub podmiotu przetwarzającego posiadającego jednostkę organizacyjną w innym państwie członkowskim. Wiodący organ nadzorczy niezwłocznie przekazuje innym organom nadzorczym, których sprawa dotyczy, stosowne informacje dotyczące danej sprawy. Niezwłocznie przedkłada innym organom, których sprawa dotyczy, nadzorczym projekt decyzji w celu uzyskania ich opinii i należytego uwzględnienia ich uwag. Jeżeli w terminie czterech tygodni od otrzymania wniosku o opinię, inny organ nadzorczy, którego sprawa dotyczy, zgłosi mający znaczenie dla sprawy i uzasadniony sprzeciw wobec projektu decyzji, wiodący organ nadzorczy – 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 w ramach mechanizmu spójności. Jeżeli wiodący organ nadzorczy zamierza przychylić się do zgłoszonego mającego znaczenie dla sprawy i uzasadnionego sprzeciwu, przedkłada innym organom nadzorczym, których sprawa dotyczy, zmieniony projekt decyzji w celu uzyskania ich opinii. Zmieniony projekt decyzji jest poddawany procedurze w terminie dwóch tygodni. Jeżeli żaden inny organ nadzorczy, którego sprawa dotyczy, nie zgłosi sprzeciwu wobec projektu decyzji przedłożonego przez wiodący organ nadzorczy, uznaje się, że wiodący organ nadzorczy i organy nadzorcze, których sprawa

[391] Państwo członkowskie, na którego terytorium została wyrządzona szkoda, naprawia taką szkodę na warunkach mających zastosowanie do szkód wyrządzonych przez jego własny personel. Państwo członkowskie organu nadzorczego oddelegowującego pracownika, którego personel wyrządził szkodę wobec osoby na terytorium innego państwa członkowskiego, zwraca temu innemu państwu członkowskiemu całą kwotę, którą zapłaciło ono osobom uprawnionym w jego imieniu. Bez uszczerbku dla możliwości dochodzenia swoich praw wobec osób trzecich i z wyjątkiem ust. 5, każde państwo członkowskie powstrzymuje się w przypadku określonym w ust. 1 od żądania odszkodowania od innego państwa członkowskiego za szkody, o których mowa w ust. 4. Zob. art. 62 ust. 5–6 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 (Dz. Urz. UE L 119 z dn. 4.05.2016, s. 1–88).

[392] Art. 62 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 (Dz. Urz. UE L 119 z dn. 4.05.2016, s. 1–88).

[393] Wiodący organ nadzorczy to 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. Zob. art. 55 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 (Dz. Urz. UE L 119 z dn. 4.05.2016, s. 1–88). Szerzej na temat wiodącego organu nadzoru zob. 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.

dotyczy, porozumiały się w sprawie projektu decyzji i są nią związane. Wiodący organ nadzorczy przyjmuje decyzję i doręcza ją odpowiednio głównej lub pojedynczej jednostce organizacyjnej administratora lub podmiotu przetwarzającego oraz informuje o decyzji inne organy nadzorcze, których sprawa dotyczy, i Europejską Radę Ochrony Danych, dołączając streszczenie stanu faktycznego i powodów decyzji. Organ nadzorczy, do którego wniesiono skargę, informuje skarżącego o decyzji. Jeżeli wiodący organ nadzorczy i organy nadzorcze, których sprawa dotyczy, porozumiały się co do oddalenia lub odrzucenia części skargi oraz co do podjęcia działań względem innych części tej skargi, dla każdej z tych części przyjmuje się odrębną decyzję. Wiodący organ nadzorczy przyjmuje decyzję w sprawie części dotyczącej działań względem administratora i doręcza ją głównej lub pojedynczej jednostce organizacyjnej administratora lub podmiotu przetwarzającego na terytorium swojego państwa członkowskiego i informuje o niej skarżącego, a organ nadzorczy skarżącego przyjmuje decyzję w sprawie części dotyczącej oddalenia lub odrzucenia tej skargi, doręcza ją skarżącemu oraz informuje o niej administratora lub podmiot przetwarzający. Po doręczeniu administratorowi lub podmiotowi przetwarzającemu decyzji wiodącego organu nadzorczego, podejmują oni niezbędne działania, by zastosować się do tej decyzji, jeżeli chodzi o czynności przetwarzania w ramach wszystkich swoich jednostek organizacyjnych w Unii. Administrator lub podmiot przetwarzający zawiadamiają wiodący organ nadzorczy o działaniach podjętych w celu zastosowania się do decyzji, ten zaś informuje o nich inne organy nadzorcze, których sprawa dotyczy. Jeżeli w wyjątkowych okolicznościach organ nadzorczy, którego sprawa dotyczy, ma powody sądzić, że istnieje pilna potrzeba podjęcia działań w celu ochrony interesów osób, których dane dotyczą, zastosowanie ma tryb pilny, o którym mowa w art. 66 RODO[394].

Zgodnie z polską ustawą o ochronie danych osobowych z 10 maja 2018 roku, w przypadkach, o których mowa w art. 61 ust. 8, art. 62 ust. 7 i art. 66 ust. 1 rozporządzenia, Prezes Urzędu może wydać postanowienie o zastosowaniu środka tymczasowego, o którym mowa w art. 70 ust. 1. 2. W postanowieniu Prezes Urzędu określa termin obowiązywania środka tymczasowego, o którym mowa w art. 70 ust. 1, nie dłuższy niż 3 miesiące. 3. Na postanowienie służy skarga do sądu administracyjnego. Wszelkie informacje kierowane przez Prezesa Urzędu do organów nadzorczych innych państw członkowskich w ramach europejskiej współpracy administracyjnej podlegają tłumaczeniu na jeden z języków urzędowych tego państwa członkowskiego lub na język angielski. W przypadku otrzymania przez Prezesa Urzędu wniosku organu nadzorczego innego państwa członkowskiego UE dotyczącego uczestnictwa we wspólnej operacji, o której mowa w art. 62 ust. 1 rozporządzenia, albo wystąpienia przez Prezesa Urzędu z takim wnioskiem, Prezes Urzędu dokonuje z organem nadzorczym innego państwa członkowskiego UE ustaleń dotyczących wspólnej operacji i niezwłocznie sporządza wykaz ustaleń[395].

[394] Art. 60 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 (Dz. Urz. UE L 119 z dn. 4.05.2016, s. 1–88).

[395] Art. 75–77 ustawy z dn. 10 maja 2018 roku o ochronie danych osobowych (Dz. U. z 2019 r., poz. 1781).

Jak wskazują statystyki dotyczące współpracy organów nadzorczych po 25 maja 2018 roku „mechanizm kompleksowej współpracy (One-Stop-Shop; OSS) wymaga współpracy wiodącego organu nadzorczego (LSA) z organami nadzorczymi, których sprawa dotyczy (CSA). Oprócz prac w celu podjęcia skoordynowanej decyzji w odniesieniu do administratora danych lub podmiotu je przetwarzającego, LSA prowadzi postępowanie i odgrywa kluczową rolę w procesie osiągania porozumienia między organami nadzorczymi, których sprawa dotyczy. Do końca 2019 roku organy nadzorcze zainicjowały 142 procedury w ramach OSS, z czego 79 zakończyło się wydaniem ostatecznej decyzji. Procedura wzajemnej pomocy umożliwia organom nadzorczym zwrócenie się z prośbą o informacje do innych organów nadzorczych lub wystąpienie z wnioskiem o zastosowanie innych środków w celu skutecznej współpracy, takich jak uprzednie zezwolenie lub postępowanie wyjaśniające. Od dnia 25 maja 2018 roku procedurę wzajemnej pomocy uruchomiono 2 542 razy. W zdecydowanej większości przypadków (2 427) były to nieformalne konsultacje; 115 stanowiły formalne wnioski. W 2019 roku organy nadzorcze nie prowadziły wspólnych operacji”[396].

Wraz z reformą przepisów powstał nowy unijny organ doradczy do spraw zgodnego z prawem przetwarzania danych osobowych – Europejska Rada Ochrony Danych Osobowych (EROD). Dotychczas działającym organem, który wydał szereg wytycznych i zaleceń wspomagających funkcjonowanie systemu ochrony danych osobowych była Grupa Robocza artykułu 29[397], dla której podstawą prawną działania był właśnie przepis art. 29 dyrektywy 95/46/WE. Można uznać, iż w ramach nowego porządku prawnego Grupę roboczą zastąpiła Europejska Rada Ochrony Danych Osobowych, której podstawą prawną funkcjonowania stał się art. 68 RODO. Organ posiada osobowość prawną i jest reprezentowany przez przewodniczącego. W skład Rady wchodzą: przewodniczący organu nadzorczego w zakresie ochrony danych osobowych z każdego państwa członkowskiego oraz Europejski Inspektor Ochrony Danych lub ich przedstawiciele. Europejska Rada Ochrony Danych obraduje pod kierownictwem przewodniczącego. Organ działa w ramach przyjętego regulaminu. Co do zasady

[396] W*spółpraca na rzecz wzmocnienia praw. Streszczenie sprawozdania rocznego za rok 2019*, Europejska Rada Ochrony Danych, https://edpb.europa.eu/sites/default/files/files/file2/edpb_annual_report_2019_-_digital_summary_pl.pdf, [dostęp: 15.07.2021].

[397] Grupa robocza ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych, zwana dalej Grupą Roboczą, powołana została na mocy art. 29 Dyrektywy 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 jako niezależny podmiot o charakterze doradczym. Grupa ta została rozwiązana 25 maja 2018 roku a w jej miejsce została powołana Europejska Rada Ochrony Danych. W skład Grupy Roboczej wchodzili przedstawiciele organu lub organów nadzorczych, powołanych przez każde Państwo Członkowskie, przedstawiciel organu lub organów ustanowionych dla instytucji i organów wspólnotowych oraz przedstawiciel Komisji. Każdy członek grupy roboczej był powoływany przez instytucję, organ lub organy, które reprezentował. W przypadku, gdyby Państwo Członkowskie powołało więcej niż jeden organ nadzorczy, organy te wyznaczały wspólnego przedstawiciela zasiadającego w Grupie Roboczej. Powyższa zasada dotyczy również organów utworzonych przez instytucje i organy wspólnotowe. Polska w Grupie Roboczej była reprezentowana przez Generalnego Inspektora Ochrony Danych Osobowych. Do zadań Grupy Roboczej należało: (a) badanie kwestii dotyczących stosowania krajowych środków przyjętych na mocy wskazanej powyżej dyrektywy, w celu przyczynienia się do jednolitego stosowania tych środków; (b) przekazywanie Komisji opinii na temat stopnia ochrony we Wspólnocie i w państwach trzecich; (c) doradzanie Komisji w sprawie wszelkich proponowanych zmian powyższej dyrektywy, dodatkowych lub szczególnych środków mających na celu zabezpieczenie praw i wolności osób fizycznych w zakresie przetwarzania danych osobowych oraz innych proponowanych środków wspólnotowych dotyczących praw i wolności; (d) wydawanie opinii na temat kodeksów postępowania opracowywanych na poziomie wspólnotowym; (e) powiadamianie Komisji w przypadku stwierdzenia występowania rozbieżności między przepisami i praktykami przyjętymi w poszczególnych Państwach Członkowskich, mogącymi mieć wpływ na równoważność ochrony danych osobowych we Wspólnocie; (f) wydawanie, z własnej inicjatywy, zaleceń we wszystkich sprawach dotyczących ochrony osób fizycznych w zakresie przetwarzania danych osobowych we Wspólnocie; (g) sporządzanie rocznego sprawozdania na temat sytuacji dotyczącej ochrony danych osobowych osób fizycznych we Wspólnocie oraz w państwach trzecich. Sprawozdania przekazywane są następnie Komisji, Parlamentowi Europejskiemu i Radzie oraz podlegają udostępnieniu opinii publicznej. Opinie i zalecenia Grupy Roboczej były przekazywane Komisji oraz komitetowi ustanowionemu na podstawie art. 31 Dyrektywy 95/46/WE. Jednocześnie, wskazać należy, iż Komisja miała obowiązek poinformować Grupę Roboczą, w drodze sprawozdania podlegającego udostępnieniu opinii publicznej oraz przekazywanego Parlamentowi Europejskiemu oraz Radzie o działaniach podjętych w odpowiedzi na jego opinie i zalecenia. Zob. *Grupa Robocza art. 29. Informacje ogólne*, Prezes Urzędu Ochrony Danych Osobowych, https://uodo.gov.pl/pl/57, [dostęp: 01.07.2021].

członkowie Rady głosują zwykłą większością głosów. W posiedzeniach EROD może brać udział również przedstawiciel Komisji Europejskiej, jednak bez prawa głosu. Pod kierownictwem przewodniczącego Rady znajduje się również sekretariat, zapewniający Radzie wsparcie analityczne, administracyjne i logistyczne. Artykuł 69 RODO nadaje Europejskiej Radzie Ochrony Danych pełną niezależność. Przepis wskazuje, że wypełniając swoje zadania, Rada nie zwraca się do nikogo o instrukcje ani ich od nikogo nie przyjmuje**.** Rada została na mocy art. 71 ust. 1 RODO zobowiązana do przygotowywania sprawozdania rocznego dotyczącego ochrony danych osobowych w Unii. Jeżeli ma to zastosowanie sprawozdanie może obejmować również ochronę danych osobowych w państwach trzecich i organizacjach międzynarodowych. EROD przekazuje sprawozdanie Parlamentowi Europejskiemu, Radzie UE i Komisji, a także podaje treść komunikatu do publicznej wiadomości.

Kompetencje Europejskiej Rady Ochrony Danych obejmują działalność na wielu płaszczyznach. Katalog uprawnień EROD pozostaje otwarty, przy czym rozporządzenie wskazuje obszerny wykaz przykładowych zadań Rady, które generalnie dzielą się w głównej mierze na monitorowanie, opiniowanie, doradzanie, rozstrzyganie sporów oraz opracowywanie wytycznych. Nadto organ ten opiniuje różne elementy działalności organów nadzorczych państw członkowskich – jak zatwierdzanie wymogów w zakresie certyfikacji czy wiążących reguł korporacyjnych, a także dawać pole do wspólnych konsultacji organów nadzorczych.

Działania EROD muszą odbywać się bez uszczerbku względem działań organów nadzorczych w zakresie ochrony danych osobowych powołanych w państwach członkowskich UE. Organ doradza Komisji Europejskiej w sprawach związanych z ochroną danych osobowych w Unii, w tym w zakresie nowelizacji RODO, oraz wymogów dotyczących wymiany informacji między administratorami, podmiotami przetwarzającymi i organami nadzorczymi dla potrzeb wiążących reguł korporacyjnych, a więc przekazywania danych poza obszar Europejskiego Obszaru Gospodarczego. Najważniejszą kompetencji Rady jest wydawanie wytycznych. Zgodnie z wykazem z art. 70 RODO, wytyczne EROD mogą dotyczyć:

- usuwania z ogólnodostępnych usług łączności łącz do danych osobowych, kopi tych danych lub ich replikacji – obejmuje to sytuacje, gdy osoba zażąda usunięcia danych na podstawie art. 17 ust. 1, a administrator upublicznił jej dane w Internecie,
- spójnego stosowania RODO – w tym zakresie EROD wytyczne wydaje z inicjatywy własnej, na wniosek jednego ze swoich członków lub Komisji Europejskiej, mogą one obejmować w szczególności wytyczne w zakresie:
  - decyzji opartych na profilowaniu – na przykład przez instytucje bankowe, czy firmy ubezpieczeniowe,
  - stwierdzania naruszenia ochrony danych osobowych i obowiązku notyfikacji naruszeń,
  - wskazywania okoliczności, które mogą powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych – na przykład przetwarzanie danych biometrycznych,

– wiążących regułach korporacyjnych,
– przekazywania danych osobowych poza Europejski Obszar Gospodarczy,
– wykonywania kompetencji i nakładania kar pieniężnych przez organy nadzorcze,
– postępowania w przypadkach zgłaszania przez osoby fizyczne naruszeń RODO[398].

Kolejnym obszarem działalności Europejskiej Rady Ochrony Danych Osobowych jest zachęcanie do sporządzania kodeksów postępowania i ustanawiania mechanizmów certyfikacji w dziedzinie ochrony danych oraz znaków jakości i oznaczeń w tej dziedzinie. Zatwierdza ona również kryteria certyfikacji i prowadzi rejestr mechanizmów certyfikacji oraz znaków jakości i oznaczeń w dziedzinie ochrony danych. EROD pełni rolę opiniodawczą – przede wszystkim względem Komisji. Opiniuje m.in.: (a) wymogi certyfikacyjne, (b) graficzne znaki jakości, (c) stopień ochrony w państwie trzecim lub organizacji międzynarodowej, (d) projekty decyzji organów nadzorczych – w ramach realizacji mechanizmu spójności, (e) kodeksy postępowań – opracowywane na poziomie unijnym.

Zadaniem Europejskiej Rady Ochrony Danych jest także prowadzenie publicznie dostępnego elektronicznego rejestru decyzji podjętych przez organy nadzorcze i wyroków sądowych w sprawach rozpatrywanych w ramach mechanizmu spójności stosowania RODO. Jednocześnie EROD ma na celu upowszechnianie wiedzy i dokumentów na temat ustawodawstwa i praktyki w dziedzinie ochrony danych w Europie i na świecie[399].

[398] *Czym jest Europejska Rada Ochrony Danych Osobowych i jakie ma zadania?*, https://www.politykabezpieczenstwa.pl/pl/a/czym-jest-europejska-rada-ochrony-danych-osobowych-i-jakie-ma-zadania, [dostęp: 01.07.2021].

[399] Szczegółową listę zadań Europejskiej Rady Ochrony Danych ustanawia art. 70 rozporządzenia, zgodnie z którym EROD z własnej inicjatywy lub w stosownych przypadkach na wniosek Komisji podejmuje w szczególności następujące działania: (a) monitoruje i zapewnia właściwe stosowanie rozporządzenia bez uszczerbku dla zadań krajowych organów nadzorczych, (b) doradza Komisji w sprawach związanych z ochroną danych osobowych w Unii, w tym w sprawie wszelkich proponowanych zmian do rozporządzenia, (c) doradza Komisji w sprawie formatu i procedur wymiany informacji między administratorami, podmiotami przetwarzającymi i organami nadzorczymi do celów wiążących reguł korporacyjnych, (d) wydaje wytyczne, zalecenia oraz określa najlepsze praktyki dotyczące usuwania z ogólnodostępnych usług łączności łącz do danych osobowych, kopi tych danych lub ich replikacji, (e) z własnej inicjatywy lub na wniosek jednego ze swoich członków lub Komisji bada wszelkie kwestie dotyczące stosowania rozporządzenia i wydaje wytyczne, zalecenia oraz określa najlepsze praktyki, by zachęcić do spójnego stosowania rozporządzenia, (f) wydaje wytyczne, zalecenia i określa najlepsze praktyki, by doprecyzować kryteria i wymogi dotyczące decyzji opartych na profilowaniu (na potrzeby art. 22 ust. 2 RODO), (g) wydaje wytyczne, zalecenia i określa najlepsze praktyki dotyczące stwierdzania naruszenia ochrony danych osobowych i określenia zbędnej zwłoki oraz szczególnych okoliczności, w których administrator lub podmiot przetwarzający mają obowiązek zgłosić naruszenie ochrony danych osobowych (h) wydaje wytyczne, zalecenia i określa najlepsze praktyki wskazujące, w jakich okolicznościach naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych (w rozumieniu art. 34 ust. 1 RODO), (i) wydaje wytyczne, zalecenia i określa najlepsze praktyki, by doprecyzować kryteria i wymogi względem przekazywania danych osobowych, które opiera się na wiążących regułach korporacyjnych stosowanych przez administratorów i na wiążących regułach korporacyjnych stosowanych przez podmioty przetwarzające, oraz inne konieczne wymogi mające zapewnić ochronę danych osobowych osób, których dane dotyczą, (zgodnie z art. 47 RODO), (j) wydaje wytyczne, zalecenia i określa najlepsze praktyki, by doprecyzować kryteria i wymogi względem przekazywania danych osobowych (na podstawie art. 49 ust. 1 RODO), (k) opracowuje wytyczne dla organów nadzorczych w sprawie stosowania środków (o których mowa w art. 58 ust. 1, 2 i 3 RODO), oraz w sprawie określania wysokości administracyjnych kar pieniężnych (zgodnie z art. 83 RODO), (l) dokonuje przeglądu praktycznego stosowania wytycznych, zaleceń i najlepszych praktyk, (m) wydaje wytyczne, zalecenia i określa najlepsze praktyki, by określić wspólne procedury postępowania w przypadkach zgłaszania przez osoby fizyczne naruszeń rozporządzenia (na potrzeby art. 54 ust. 2 RODO), (n) zachęca do sporządzania kodeksów postępowania oraz do ustanawiania mechanizmów certyfikacji w dziedzinie ochrony danych oraz znaków jakości i oznaczeń w tej dziedzinie (zgodnie z art. 40 i 42 RODO), (o) akredytuje podmioty certyfikujące i dokonuje okresowego przeglądu certyfikacji (zgodnie z art. 43 RODO) oraz prowadzi publiczny rejestr podmiotów akredytowanych (zgodnie z art. 43 ust. 6 RODO) i administratorów i podmiotów przetwarzających akredytowanych (zgodnie z art. 42 ust. 7 RODO), mających siedzibę w państwach trzecich, (p) precyzuje wymogi z myślą o akredytacji podmiotów certyfikujących (zgodnie z art. 42 RODO), (r) udziela Komisji opinii w sprawie wymogów certyfikacyjnych (o których mowa w art. 43 ust. 8 RODO), (s) udziela Komisji opinii w sprawie znaków graficznych (o których mowa w art. 12 ust. 7 RODO), (t) udziela Komisji opinii na potrzeby oceny, czy stopień ochrony w państwie trzecim lub organizacji międzynarodowej jest odpowiedni, w tym na potrzeby oceny, czy państwo trzecie, terytorium, określony sektor lub określone sektory w tym państwie trzecim lub organizacja międzynarodowa nie przestały zapewniać odpowiedniego stopnia ochrony (w tym celu Komisja udostępnia Europejskiej Radzie Ochrony Danych wszelką niezbędną dokumentację, w tym korespondencję z rządem państwa trzeciego w odniesieniu do tego państwa trzeciego, terytorium lub określonego sektora lub korespondencję z organizacją międzynarodową), (u) wydaje opinie w sprawie projektów decyzji zgłoszonych przez organy nadzorcze zgodnie z mechanizmem spójności w sprawach przedłożonych jej (zgodnie z art. 64 ust. 2 RODO) oraz wydaje wiążące decyzje, w tym w sprawach (o których mowa w art. 66 RODO), (w) upowszechnia współpracę oraz skuteczną dwustronną i wielostronną wymianę informacji i dobrych praktyk między organami nadzorczymi, (x) upowszechnia wspólne programy szkoleń oraz ułatwia wymianę personelu między organami nadzorczymi, a w stosownych przypadkach – z organami nadzorczymi państw trzecich lub organizacji międzynarodowych, (y) upowszechnia wymianę wiedzy i dokumentów na temat ustawodawstwa i praktyki w dziedzinie ochrony danych z organami nadzorczymi odpowiedzialnymi za ochronę danych na świecie, (z) wydaje opinie na temat kodeksów postępowania opracowywanych na szczeblu Unii (zgodnie z art. 40 ust. 9 RODO), oraz prowadzi publicznie dostępny elektroniczny rejestr decyzji podjętych przez organy nadzorcze i wyroków sądowych w sprawach rozpatrywanych w ramach mechanizmu spójności. Art. 70 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia

Właściwą procedurę rozstrzygania sporów przez Europejską Radę Ochrony Danych reguluje dokładnie przepis art. 65 rozporządzenia, w myśl którego, aby w poszczególnych sytuacjach zapewnić właściwe i spójne stosowanie tego aktu prawnego, Europejska Rada Ochrony Danych wyposażono w kompetencje do przyjmowania wiążących decyzji[400] w następujących przypadkach:

a) jeżeli organ nadzorczy, którego sprawa dotyczy, zgłosił mający znaczenie dla sprawy i uzasadniony sprzeciw wobec projektu decyzji wiodącego organu nadzorczego, a wiodący organ nadzorczy nie przychylił się do tego sprzeciwu lub odrzucił taki sprzeciw jako niemający znaczenia dla sprawy lub nieuzasadniony. Wiążąca decyzja dotyczy wszystkich spraw, które są przedmiotem mającego znaczenie dla sprawy i uzasadnionego sprzeciwu, w szczególności dotyczy tego, czy doszło do naruszenia rozporządzenia;
b) jeżeli panują sprzeczne opinie co do tego, który z organów nadzorczych, których sprawa dotyczy, jest właściwy względem głównej jednostki organizacyjnej;
c) jeżeli właściwy organ nadzorczy nie wystąpił o opinię do Europejskiej Rady Ochrony Danych, lub nie zastosował się do opinii Europejskiej Rady Ochrony Danych wydanej zgodnie z art. 64; w takim przypadku organ nadzorczy, którego sprawa dotyczy, lub Komisja mogą zgłosić sprawę Europejskiej Radzie Ochrony Danych[401].

Decyzję Europejska Rada Ochrony Danych przyjmuje większością dwóch trzecich głosów swoich członków w terminie miesiąca od wpłynięcia sprawy. Ze względu na złożony charakter sprawy termin ten można przedłużyć o miesiąc. Decyzja zostaje wraz z uzasadnieniem skierowana do wiodącego organu nadzorczego i wszystkich organów nadzorczych, których sprawa dotyczy, i jest dla nich wiążąca[402].

Przewodniczący EROD bez zbędnej zwłoki notyfikuje decyzję organom nadzorczym, których sprawa dotyczy, a decyzja jest niezwłocznie publikowana na stronie internetowej EROD. Jednocześnie informuje o niej Komisję. Bez zbędnej zwłoki i najpóźniej w terminie miesiąca po notyfikowaniu przez Europejską Radę Ochrony Danych swojej decyzji, wiodący organ nadzorczy lub w stosownym przypadku organ nadzorczy, do którego wniesiono skargę, przyjmuje ostateczną decyzję na podstawie decyzji. Wiodący organ nadzorczy lub w stosownym przypadku organ nadzorczy, do którego wniesiono skargę, informuje Europejską Radę Ochrony Danych o terminie, w którym doręczono ostateczną decyzję odpowiednio administratorowi lub podmiotowi przetwarzającemu oraz osobie, której dane dotyczą[403].

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).

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

[401] Art. 65 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 (Dz. Urz. UE L 119 z dn. 4.05.2016, s. 1–88).

[402] Jeżeli Europejska Rada Ochrony Danych nie jest w stanie przyjąć decyzji w powyższych terminach, przyjmuje decyzję w terminie dwóch tygodni po upłynięciu drugiego miesiąca, zwykłą większością głosów swoich członków. Jeżeli głosy członków Europejskiej Rady Ochrony Danych rozkładają się po równo, decyduje głos przewodniczącego. Przed upływem powyższych terminów organy nadzorcze, których sprawa dotyczy, nie przyjmują decyzji w sprawie przedłożonej Europejskiej Radzie Ochrony Danych na mocy ust. 1. Zob. art. 65 ust. 3–4 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 (Dz. Urz. UE L 119 z dn. 4.05.2016, s. 1–88).

[403] Ostateczna decyzja organów nadzorczych, których sprawa dotyczy, zostaje przyjęta w trybie art. 60 ust. 7, 8 i 9 i zawiera informacje o decyzji, o której mowa w ust. 1 niniejszego artykułu, i wskazuje, że decyzja, o której mowa w tym ustępie, zostanie opublikowana na stronie internetowej Europejskiej Rady

Przepis art. 66 rozporządzeniu ustanawia jednocześnie tryb pilny. W wyjątkowych okolicznościach, jeżeli organ nadzorczy, którego sprawa dotyczy, uzna, że istnieje pilna potrzeba podjęcia działań w celu ochrony praw i wolności osób, których dane dotyczą, może w drodze odstępstwa od mechanizmu spójności (o którym mowa w art. 63, 64 i 65), lub od procedury (o której mowa w art. 60), niezwłocznie przyjąć środki tymczasowe mające na terytorium jego państwa członkowskiego wywołać skutki prawne przez określony okres, nieprzekraczający trzech miesięcy. Organ nadzorczy niezwłocznie informuje o tych środkach i o powodach ich przyjęcia pozostałe organy nadzorcze, których sprawa dotyczy, Europejską Radę Ochrony Danych i Komisję. Jeżeli organ nadzorczy zastosował taki środek i uznaje, że należy pilnie przyjąć środki o charakterze ostatecznym, może zwrócić się z wnioskiem o pilne wydanie opinii lub wiążącej decyzji do Europejskiej Rady Ochrony Danych, uzasadniając swój wniosek o taką opinię lub decyzję. Organ nadzorczy może zwrócić się do EROD z wnioskiem o pilne wydanie opinii lub w stosownym przypadku wiążącej decyzji, uzasadniając swój wniosek o taką opinię lub decyzję, w tym uzasadniając pilną potrzebę działań – jeżeli właściwy organ nadzorczy nie zastosował odpowiedniego środka w sytuacji, w której istnieje pilna potrzeba podjęcia działań w celu ochrony praw i wolności osób, których dane dotyczą. Europejska Rada Ochrony Danych przyjmuje opinię lub wiążącą decyzję wydawane w trybie pilnym, w terminie dwóch tygodni zwykłą większością głosów swoich członków[404].

W swoim sprawozdaniu rocznym za 2019 rok Europejska Rada Ochrony Danych informuje, że przyjęła pięć nowych wytycznych, mających na celu doprecyzowanie zakresu przepisów RODO. Ponadto, w 2019 r., po przeprowadzeniu konsultacji publicznych, trzy dokumenty zawierające wytyczne przyjęte w 2018 r. zostały zatwierdzone przez EROD w ostatecznej formie. W 2019 r. EROD wydała także 16 opinii w ramach mechanizmu spójności. Jako organ rozstrzygający spory i wydający wiążące decyzje, od dnia 25 maja 2018 roku do końca 2019 roku, EROD nie wszczęła żadnej procedury rozstrzygania sporów, co pozwala sądzić, że w tym czasie organy nadzorcze były w stanie osiągnąć porozumienie w sprawie wszystkich bieżących spraw transgranicznych. EROD doradzało także Komisji Europejskiej we wszelkich kwestiach związanych z ochroną danych osobowych, w tym w sprawie adekwatności stopnia ochrony danych w państwach trzecich lub organizacjach międzynarodowych. W ramach art. 42 rozporządzenia 2018/1725 w kwestii konsultacji w sprawie aktów ustawodawczych w 2019 roku EROD i Europejski Inspektor Ochrony Danych wydały wspólną opinię na temat aspektów ochrony danych w ramach europejskiej infrastruktury usług cyfrowych w dziedzinie e-zdrowia. Również ta opinia została wydana na wniosek DG SANTE. W 2019 r. Rada wydała także dwa oświadczenia. W 2019 roku, po wstępnym przyjęciu wytycznych EROD,

Ochrony Danych. Art. 65 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 (Dz. Urz. UE L 119 z dn. 4.05.2016, s. 1–88).

[404] Art. 66 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 (Dz. Urz. UE L 119 z dn. 4.05.2016, s. 1–88).

zorganizowało pięć konsultacji publicznych oraz trzy wydarzenia, poświęcone zmienionej dyrektywie w sprawie usług płatniczych (PSD2), koncepcji i odpowiedzialności administratorów i podmiotów przetwarzających oraz praw osób, których dane dotyczą. W raporcie za 2019 wskazuje się na wyzwania której stoją zarówno przed EROD, jak i organami nadzorczymi państw członkowskich. „Różnorodność krajowych przepisów proceduralnych ma wpływ na mechanizm współpracy, ze względu na różnice dotyczące procedur rozpatrywania skarg, sytuacji stron w postępowaniach, kryteriów dopuszczalności, czasu trwania postępowań, terminów itd. Ponadto skuteczne stosowanie uprawnień i zadań powierzonych organom nadzorczym na mocy RODO zależy w dużej mierze od dostępnych im zasobów. Dotyczy to w szczególności mechanizmu kompleksowej współpracy (OneStop-Shop), którego powodzenie zależy od wysiłku organów nadzorczych i czasu, jaki mogą one poświęcić współpracy i poszczególnym sprawom. Pomimo tych wyzwań EROD jest przekonana, że współpraca organów nadzorczych doprowadzi do stworzenia wspólnej kultury ochrony danych i spójnych praktyk kontrolnych”[405].

Jak wskazują historyczne już doświadczenia Grupy Roboczej art. 29 oraz bieżąca działalność Europejskiej Rady Ochrony Danych, funkcjonowanie tego typu organów ma duży wpływ na stosowanie RODO. Lata funkcjonowania Grupy Roboczej pokazały, jak ważne mogą być ustalane wspólnie na poziomie międzynarodowym[406], wytyczne w zakresie bezpiecznego przetwarzania danych osobowych. Należy pamiętać bowiem, że w możliwym do zastosowania zakresie nie utraciły mocy wytyczne przyjęte przez Grupę Roboczą art. 29. Tym samym funkcjonowanie EROD, jako unijnego organu doradczego w zakresie ochrony danych osobowych, należy traktować jako kontynuację pracy Grupy Roboczej art. 29[407].

Uprzednie konsultacje, kodeksy postępowania, certyfikacja i akredytacja

Wystarczające gwarancje przestrzegania standardów ochrony danych osobowych administrator, jak i procesor może wykazać między innymi poprzez nowe instrumenty wprowadzone przez RODO, tj. stosowanie zatwierdzonego kodeksu postępowania, o którym mowa w art. 40, lub zatwierdzonego mechanizmu certyfikacji, o którym mowa w art. 42[408].

Po pierwsze rozporządzenie wprowadziło do sytemu prawnego ochrony danych osobowych nieznany wcześniej instrument polegający na przeprowadzaniu uprzednich konsultacji

[405] W*spółpraca na rzecz wzmocnienia praw. Streszczenie sprawozdania rocznego za rok 2019*, Europejska Rada Ochrony Danych, https://edpb.europa.eu/sites/default/files/files/file2/edpb_annual_report_2019_-_digital_summary_pl.pdf, [dostęp: 15.07.2021].

[406] Współpraca międzynarodowa w obszarze ochrony danych osobowych odbywa się w ramach takich organizacji i inicjatyw międzynarodowych jak m.in.: Europejski Inspektor Ochrony Danych Osobowych, Rada Europy, Grupa Państw Europy Środkowej i Wschodniej, Grupa Berlińska, Grupa ds. Koordynacji Nadzoru nad Systemem Eurodac, Rada Współpracy Europolu, Grupa ds. Koordynacji Nadzoru nad Wizowym System Informacyjnym, Wspólny Organ Nadzorczy ds. Celnych, Grupa ds. Koordynacji Nadzoru nad Systemem Informacyjnym Schengen, w ramach realizacji Funduszy Europejskich, TFTP, Schengen, System IMI, Tarcza Prywatności, Global Privacy Assembly (GPA), Global Privacy Enforcement Network (GPEN), Organy Innych Państw, Agencja Praw Podstawowych. Szerzej zob. *Współpraca międzynarodowa*, Urząd Ochrony Danych Osobowych, https://uodo.gov.pl/p/wspolpraca, [dostęp: 01.07.2021].

[407] Zob. 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.

[408] Przykładowo przekazanie danych do państwa trzeciego lub organizacji międzynarodowej może nastąpić, na podstawie stosownej decyzji Komisji Europejskiej. W braku decyzji przekazanie danych do państwa trzeciego może nastąpić, m.in. jeżeli zostały zapewnione odpowiednie zabezpieczenia ochrony danych niewymagające uzyskania specjalnego zezwolenia ze strony organu nadzorczego, za pomocą jednego z następujących instrumentów: (a) zatwierdzonego kodeksu postępowania lub (b) zatwierdzonego mechanizmu certyfikacji. Zob. art. 40 i 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 oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. UE L 119 z dn. 4.05.2016, s. 1–88).

z organem nadzorczym. I tak, jeżeli ocena skutków dla ochrony danych, wskaże, że przy braku lub niedostatecznym poziomie planowanych zabezpieczeń środków bezpieczeństwa oraz mechanizmów minimalizujących ryzyko przetwarzanie powodowałoby wysokie ryzyko naruszenia praw lub wolności osób fizycznych, a administrator uznaje, że ryzyka tego nie da się zminimalizować środkami rozsądnymi z punktu widzenia dostępnych technologii i kosztów wdrożenia, to przed rozpoczęciem przetwarzania zobowiązany jest do przeprowadzenia konsultacji z organem nadzorczym[409]. W tym zakresie przedstawia:

a) odpowiednie obowiązki podmiotów uczestniczących w przetwarzaniu, w szczególności w przypadku przetwarzania w ramach grupy przedsiębiorstw,
b) cele i sposoby zamierzonego przetwarzania,
c) środki i zabezpieczenia mające chronić prawa i wolności osób, których dane dotyczą,
d) dane kontaktowe Inspektora Ochrony Danych,
e) ocenę skutków dla ochrony danych.

Projektując operacje przetwarzania, wymagające uprzednich konsultacji, Administrator uwzględnia określone w art. 36 ust. 2 rozporządzenia terminy na udzielenie przez organ nadzorczy zaleceń lub podjęcie środków naprawczych. Organ, w ramach instrumentu uprzednich konsultacji, formułuje stosowne zalecenia. Administrator uwzględnia zalecenia organu nadzorczego wydane na skutek uprzednich konsultacji.

Po drugie rozporządzenie wprowadziło podstawy prawne dla tworzenia tzw. kodeksów postępowania mających pomóc podmiotom z konkretnego sektora w interpretacji i stosowaniu przepisów. Elastyczność RODO z jednej strony daje administratorom wiele swobody co do stosowanych rozwiązań. Z drugiej strony wymusza podejście branżowe, dopasowujące organizację systemu ochrony danych do specyfiki prowadzonej działalności. Z pomocą przychodzą wspomniane (dobrowolne) kodeksy postępowania, które doprecyzowują i ułatwiają właściwe wdrożenie systemów ODO w danej branży.

Warunkiem przyjęcia kodeksu postępowania jest przedłożenie jego projektu organowi nadzorczemu do zatwierdzenia. Projekt taki musi spełniać wymogi określone w RODO i ustawie o ochronie danych osobowych, jak również te określone w Wytycznych EROD nr 1/2019 dotyczących kodeksów postępowania i podmiotów monitorujących[410]. Poprawnie złożony wniosek o zatwierdzenie projektu kodeksu postępowania powinien zawierać informację o przeprowadzonych konsultacjach oraz ich wyniku. Konsultacje muszą zostać przeprowadzone przed złożeniem wniosku o zatwierdzenie kodeksu[411]. W pierwszej kolejności

[409] Motyw 94 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 (Dz. Urz. UE L 119 z dn. 4.05.2016, s. 1–88).

[410] Wytyczne 1/2019 dotyczące kodeksów postępowania i podmiotów monitorujących zgodnie z rozporządzeniem 2016/679, Europejska Rada Ochrony Danych, wersja 2.0 z dn. 4 czerwca 2019 r.

[411] Informacje o przeprowadzonych konsultacjach muszą obejmować najważniejsze wnioski wraz z odniesieniem projektodawców do przedstawionych stanowisk (raport z konsultacji). Konsultacje powinny zostać przeprowadzone w możliwie szerokim zakresie przy wykorzystaniu wszelkich możliwych kanałów komunikacji, w tym np. strony internetowej, prasy branżowej czy też pism kierowanych wprost do zainteresowanych podmiotów i organizacji. Przedłożenie wniosku o zatwierdzenie kodeksu postępowania wiąże się również z obowiązkiem uiszczenia opłaty skarbowej w wysokości 10 złotych. Opłatę należy uiścić na właściwe konto Dzielnicy Śródmieście m.st. Warszawy. W związku z tym że RODO nie określa, jak dokładnie ma wyglądać

organ nadzorczy bada, czy przedłożony projekt spełnia wymogi formalne oraz kryteria dopuszczalności. Następnie dokonywana jest ocena przedłożonego projektu w oparciu o kryteria zatwierdzania kodeksów. Na tym etapie dopuszczalne są ewentualne modyfikacje. Procedura swój finał znajduje w zatwierdzeniu kodeksu postępowania w formie decyzji administracyjnej[412]. Należy mieć na uwadze, że ustawodawca europejski przewidział także możliwość rozszerzenia zakresu ważności terytorialnej danego kodeksu, poprzez zarejestrowanie go przy europejskim organie nadzorczym[413].

Do obowiązywania kodeksu potrzeba jeszcze wydania przez urząd nadzoru akredytacji dla niezależnego podmiotu, którego zadaniem jest monitorowanie przestrzegania kodeksu[414]. Podmiot ten musi zostać akredytowany przez organ nadzorczy jeszcze przed zatwierdzeniem kodeksu postępowania[415]. Organ nadzorczy dokonuje akredytacji podmiotu monitorującego dany kodeks postępowania na podstawie przepisów RODO (art. 41), Wytycznych EROD nr 1/2019, ustawy o ochronie danych osobowych (art. 27) oraz Wymogów akredytacji podmiotów monitorujących kodeksy (dokument został już opracowany przez Prezesa Urzędu Ochrony Danych Osobowych i zaopiniowany przez EROD)[416].

Przystąpienie do stosowania kodeksu postępowania wiąże się z korzyściami. Po pierwsze daje to gwarancję pewności stosowania określonych rozwiązań. Można również liczyć na nadzór niezależnego podmiotu monitorującego (w praktyce np. kontrola podmiotu, czy też rozpatrywanie skarg osób, których dane dotyczą, mogą odbywać się bez udziału organu nadzorczego). Niewątpliwą korzyścią ze stosowania kodeksu jest także swoista ochrona w kontekście ewentualnych kar pieniężnych[417].

procedura zatwierdzania kodeksów, prowadzona przez UODO praktyka przybiera formę spotkań z autorami projektów w celu uzyskania wyjaśnień, jak i przekazania ewentualnych wątpliwości czy wskazania problematycznych kwestii. Zob. *Procedura zatwierdzania kodeksu*, Urząd Ochrony Danych Osobowych, https://uodo.gov.pl/pl/426/1103, [dostęp:18.08.2021].

[412] Przyjęty kodeks postępowania – EU Data Protection Code of Conduct for Cloud Service Providers („EU Cloud CoC") – konkretyzuje przepisy RODO i określa dobre praktyki dla dostawców usług w chmurze (IaaS, PaaS, SaaS). Jako podmiot monitorujący przestrzeganie kodeksu został wybrany Scope Europe. Zob. M. Madecki, *Pierwszy zatwierdzony kodeks postępowania RODO*, https://rodoradar.pl/pierwszy-zatwierdzony-kodeks-postepowania-rodo/, [dostęp:18.08.2021].

[413] Procedury zatwierdzania kodeksu krajowego i europejskiego (transgranicznego) są do siebie zbliżone. Ważne jest określenie wprost w projekcie kodeksu, czy kodeks jest jedynie krajowy, czy dotyczyć będzie również przetwarzania danych osobowych w innych państwach członkowskich UE. Kodeks transgraniczny musi bowiem spełniać dodatkowe wymagania formalne, np. w kontekście wersji językowych. Jego projekt – odmiennie niż w przypadku kodeksów krajowych – musi zostać również zaopiniowany przez EROD i Komisję Europejską. Zob. *Procedura zatwierdzania kodeksu*, Urząd Ochrony Danych Osobowych, https://uodo.gov.pl/pl/426/1103, [dostęp:18.08.2021].

[414] Podmiot monitorujący przestrzeganie danego kodeksu musi spełniać określone wymagania, jak np. posiadanie fachowej wiedzy w dziedzinie będącej przedmiotem kodeksu, zachowanie niezależności, dysponowanie procedurami pozwalającymi ocenić, czy administratorzy przestrzegają kodeksu oraz takimi, które pozwolą mu rozpatrywać skargi na naruszenia kodeksu. Podmiot monitorujący musi też spełnić wymogi akredytacji, które są określone przez UODO i zaopiniowane przez Europejską Radę Ochrony Danych w celu zapewnienia spójności stosowania przepisów RODO we wszystkich państwach członkowskich. Zob. *Monitorowanie kodeksów. Jak stworzyć odpowiedni mechanizm? Na co zwrócić uwagę a czego unikać*, Urząd Ochrony Danych Osobowych, https://uodo.gov.pl/pl/138/2203, [dostęp:18.08.2021].

[415] W marcu 2021 roku Prezes UODO pozytywnie zaopiniował pierwsze dwa kodeksy, oba z obszaru ochrony zdrowia: (1) Kodeks dla małych placówek medycznych przygotowany przez Porozumienie Zielonogórskie oraz (2) Kodeks dla sektora ochrony zdrowia przygotowany przez Polską Federację Szpitali. Zob. M. Popiel, *Pozytywna opinia dla pierwszych kodeksów postępowania RODO*, https://panoptykon.org/pierwsze-kodeksy-rodo-zatwierdzone, [dostęp:18.08.2021]. Na opinię Prezesa UODO czeka jeszcze kilka innych projektów kodeksów, które zostały przedłożone organowi nadzorczemu do zatwierdzenia przez: (a) Związek Rewizyjny Spółdzielni Mieszkaniowych RP, (b) Krajową Izbę Doradców Podatkowych, (c) Związek Pracodawców Organizacja Firm Badania Opinii i Rynku, (d) Polską Radę Centrów Handlowych, (5) Sieć Badawczą Łukasiewicz – PORT Polski Ośrodek Rozwoju Technologii. Lista ta nie obejmuje projektów kodeksów postępowania, które nie zostały jeszcze przedłożone organowi nadzorczemu do zatwierdzenia, ale trwają nad nimi prace: (1) Kodeks postępowania i dobrych praktyk w zakresie ochrony danych osobowych w działaniach marketingu bezpośredniego – Polskie Stowarzyszenie Marketingu SMB, (2) Kodeks postępowania w zakresie ochrony danych osobowych (dla Uczelni Medycznych) – Uczelnie Członkowskie Konferencji Rektorów Akademickich Uczelni Medycznych, (3) Kodeks dotyczący zasad przetwarzania danych osobowych gości hotelowych – Izba Gospodarcza Hotelarstwa Polskiego, (4) Kodeks postępowania ochrony danych osobowych dla branży wodociągowo-kanalizacyjnej – IGWP Izba Gospodarcza „Wodociągi Polskie", (5) Kodeks postępowania dla branży badań medycznych – INFARMA. Związek Pracodawców Innowacyjnych Firm Farmaceutycznych. Zob. *Złożone wnioski o zatwierdzenie kodeksów*, Urząd Ochrony Danych Osobowych, https://uodo.gov.pl/pl/426/1109, [dostęp:18.08.2021].

[416] Konieczność wskazania podmiotu monitorującego nie dotyczy kodeksów mających mieć zastosowanie wyłącznie do przetwarzania danych przez organy publiczne. Jednak nie oznacza to braku nadzoru – monitorowanie wykonuje wtedy inny podmiot sprawujący nadzór nad takim podmiotem publicznym. Zob. *Kodeksy postępowania muszą spełniać określone wymagania*, Urząd Ochrony Danych Osobowych, https://uodo.gov.pl/pl/138/1858, [dostęp:18.08.2021].

[417] K. Sobczak, *RODO: Osiem projektów kodeksów, ale żaden jeszcze nie zatwierdzony*, https://www.prawo.pl/biznes/kodeksy-rodo-osiem-projektow-ale-zaden-jeszcze-nie-zatwierdzony,505991.html, [dostęp:18.08.2021].

Po trzecie rozporządzenie uregulowało nową możliwość certyfikowania wewnętrznych systemów ochrony danych osobowych konkretnych administratorów danych[418]. Cel wprowadzenia certyfikacji oddaje bardzo dokładnie motyw 100 preambuły do RODO. Wskazuje on, iż aby zwiększyć przejrzystość i poprawić przestrzeganie rozporządzenia, należy zachęcać do ustanowienia mechanizmów certyfikacji oraz do wprowadzenia znaków jakości i oznaczeń, pozwalając w ten sposób osobom, których dane dotyczą, szybko ocenić stopień ochrony danych, której podlegają stosowne produkty i usługi.

Art. 42 ust. 5 RODO stanowi, że certyfikacja odbywa się na podstawie kryteriów certyfikacji, które powinien zatwierdzić właściwy organ nadzorczy[419]. Listę podmiotów, które uzyskały certyfikat publikuje również na swojej stronie internetowej Prezes UODO. Certyfikaty udzielane są bądź bezpośrednio przez organ nadzorczy, bądź przez akredytowane podmioty certyfikujące[420]. Aby dana instytucja uzyskała status podmiotu certyfikującego (i w konsekwencji możliwość przyznawania certyfikatów), musi uzyskać odpowiednią akredytację, udzielaną przez organ nadzorczy lub krajową jednostkę akredytującą. Analogicznie do kryteriów certyfikacji wprowadzono tzw. wymogi akredytacji, które z kolei stanowią wytyczne dla podmiotów, które chcą wydawać certyfikaty. W odniesieniu do tych wymogów Europejska Rada Ochrony Danych wydała Wytyczne 4/2018 w sprawie akredytacji jednostek certyfikujących[421]. Prezes jest zobowiązany do opublikowania na swojej stronie internetowej kryteriów akredytacji. Kompetencję do akredytacji podmiotów certyfikujących przyznano Polskiemu Centrum Akredytacji, które o każdorazowym udzieleniu akredytacji musi zawiadomić Prezesa UODO. Sam proces certyfikacji polega na:

1) złożeniu pisemnie lub elektronicznie wniosku o certyfikację zawierającego co najmniej:
   – nazwę podmiotu (albo imię i nazwisko) oraz wskazanie adresu siedziby,
   – informacje potwierdzające spełnianie kryteriów certyfikacji,
   – wskazanie zakresu wnioskowanej certyfikacji;
2) zbadaniu spełniania kryteriów;

[418] Certyfikat może być przyznany na rzecz podmiotu, który złożył stosowny wniosek. Do wniosku dołącza się dokumenty potwierdzające spełnianie kryteriów certyfikacji albo ich kopie. W przypadku gdy certyfikat ma zostać udzielony bezpośrednio przez Prezesa UODO, wniosek podlega opłacie w wysokości ustalonej przez Prezesa Urzędu na podstawie zakresu certyfikacji, przewidywanego przebiegu i długości postępowania certyfikującego oraz kosztu pracy pracownika wykonującego czynności związane z certyfikacją. Maksymalna wysokość opłaty nie może przekroczyć czterokrotności przeciętnego wynagrodzenia w gospodarce narodowej w roku kalendarzowym poprzedzającym rok złożenia wniosku o certyfikację, ogłaszanego przez Prezesa Głównego Urzędu Statystycznego. Zob. art. 26 ustawy o ochronie danych osobowych (t.j. Dz.U. z 2019 r., poz. 1781).

[419] Pracę nad wytycznymi kryteriów certyfikacji w Polsce trwają. Należy zauważyć, że Prezes UODO nie udostępnia informacji na temat certyfikatów. Wskazuje się, że certyfikaty będą wydawane dopiero po zakończeniu prac nad procesem oceny certyfikatów prowadzonych przez Europejską Radę Ochrony Danych. Tymczasem EROD wydała pierwszą opinię w sprawie kryteriów certyfikacji. Opinię przyjęto 1 lutego 2022 roku podczas 60. posiedzenia plenarnego. Opinia EROD dotyczy projektu decyzji luksemburskiego organu nadzorczego w sprawie kryteriów certyfikacji RODO-CARPA. Zob. *Pierwsza opinia EROD w sprawie kryteriów certyfikacji*, Urząd Ochrony Danych Osobowych, https://uodo.gov.pl/pl/138/2299, [dostęp:6.02.2022].

[420] Od podmiotów certyfikujących wymaga się – oprócz niezależności i fachowej wiedzy – także opracowania oraz stosowania procedur wydawania, okresowego przeglądu i cofania certyfikacji, znaków jakości i oznaczeń w dziedzinie ochrony danych, Podmioty te powinny także dysponować procedurami i strukturami, które pozwalają rozpatrywać skargi na naruszenie warunków certyfikacji lub na sposób wdrożenia lub wdrażania certyfikacji przez administratora lub podmiot przetwarzający. Zob. S. Osowska, *Akredytacja i certyfikacja na gruncie RODO*, https://cowprawiepiszczy.com/2019/04/akredytacja-i-certyfikacja-na-gruncie-rodo/, [dostęp: 18.08.2021]

[421] Wytyczne 4/2018 w sprawie akredytacji podmiotów certyfikujących na podstawie art. 43 ogólnego rozporządzenia o ochronie danych (2016/679), Europejska Rada Ochrony Danych, wersja 3.0 z 4 czerwca 2019 r. Pomimo, iż kształt wymogów akredytacji wciąż nie jest znany, wiadomym jest, że będą one jedynie uzupełnieniem normy ISO 17065/2012. Podmioty, które myślą o uzyskaniu statutu „podmiotu akredytowanego" powinny mieć wdrożone w swojej firmie normy ISO 17065/2012. S. Osowska, *Akredytacja i certyfikacja na gruncie RODO*, https://cowprawiepiszczy.com/2019/04/akredytacja-i-certyfikacja-na-gruncie-rodo/, [dostęp: 18.08.2021].

3) zawiadomieniu wnioskodawcy w terminie nie dłuższym niż trzy miesiące od dnia złożenia wniosku o dokonaniu albo odmowie dokonania certyfikacji[422].

Nadanie lub odmowa nadania certyfikatu powinno nastąpić w terminie 3 miesięcy od dnia złożenia stosownego wniosku przez administratora danych lub podmiot przetwarzający. Certyfikat udzielany jest na określony czas, przy czym RODO wskazuje, że jest to okres do trzech lat[423]. W sytuacji utraty spełniania kryteriów dotyczące certyfikacji, podmiot który jej udzielił ma prawo do cofnięcia certyfikatu. Sam Prezes Urzędu może również dokonywać czynności sprawdzających polegających na możliwości weryfikacji, czy podmiot który otrzymał certyfikat przestrzega kryteriów certyfikacji. Po upływie czasu, na który certyfikat został wystawiony, konieczne jest wystąpienie o odnowienie certyfikatu[424].

Certyfikacja jest dobrowolna i fakultatywna. Należy mieć na uwadze, że uzyskanie certyfikatu po pierwsze nie zwalnia z obowiązku stosowania przepisów rozporządzenia, po drugie nie wpływa na możliwość kontrolowania danego podmiotu przez organ nadzorczy. Tym samym generalne obowiązki wynikające z RODO w odniesieniu do podmiotu, który uzyskał certyfikat, są analogiczne do tych, które obciążają innych administratorów i podmioty przetwarzające. Zastanawiając się zatem na korzyściami wynikającymi z posiadania certyfikatu należy chociażby wspomnieć o budowaniu zaufania klientów. Jest to instrument przeznaczony dla podmiotów, które chciałyby wykazać publicznie, że spełniają odpowiednie standardy zabezpieczenia. Ponadto, niewątpliwą korzyścią posiadania certyfikatu jest jego wpływ na wysokość administracyjnej kary pieniężnej w sytuacji naruszenia przez administratora przepisów. Zgodnie bowiem z art. 83 ust. 2 lit. j RODO – krajowy organ nadzorczy, decydując się na nałożenie kary pieniężnej, przy ustalaniu jej wysokości musi wziąć pod uwagę okoliczność, czy podmiot dopuszczający się naruszeń stosował zatwierdzone mechanizmy certyfikacji. Co za tym idzie, jednostka posiadająca certyfikat będzie mogła na przykład liczyć na ewentualny łagodniejszy wymiar kary[425].

Pomimo obowiązywania już kilka lat ww. możliwości, narzędzia te pozostają praktycznie martwe. Wynik dwóch zarejestrowanych kodeksów w Polsce w okresie 4 lat stanowi doskonałą ilustrację problemu.

[422] Art. 17 ustawy o ochronie danych osobowych (t.j. Dz.U. z 2019 r., poz. 1781).
[423] Dokument certyfikatu zawiera oznaczenie podmiotu, który otrzymał certyfikat, nazwie podmiotu dokonującego certyfikacji oraz wskazanie adresu jego siedziby, numeru lub oznaczeniu certyfikatu, zakresie dokonanej certyfikacji, wskazaniu okresu na jaki został udzielony certyfikat oraz datę wydania i podpis podmiotu dokonującego certyfikacji lub osoby przez niego upoważnionej. Art. 21 ustawy o ochronie danych osobowych (t.j. Dz.U. z 2019 r., poz. 1781).
[424] Zob. *Certyfikat zgodności z RODO*, https://lexdigital.pl/certyfikat-zgodnosci-z-rodo, [dostęp: 18.08.2021].
[425] Mechanizm certyfikacji może odgrywać istotną rolę w zamówienia publicznych, z uwagi na fakt, iż zamawiający w Specyfikacji Warunków Zamówienia (SWZ) będzie mógł wymaga od wykonawców posiadania certyfikatu poświadczającego zgodność przetwarzania danych osobowych zgodnie z wymogami RODO. Zob. K. Sobczak, *RODO – certyfikacja to obowiązek i korzyści dla administratora danych*, https://www.prawo.pl/prawnicy-sady/rodo-certyfikacja-to-obowiazek-i-korzysci-dla-administratora-danych,74396.html, [dostęp: 18.08.2021].

Podsumowanie

Kompleksowa reforma systemu ochrony danych osobowych była oczywistą próbą wyjścia na przeciw zarzutom związanym z brakiem spójnego, ujednoliconego porządku prawnego GDPR na terenie UE, w sytuacji wykładniczego przybywania przepływów informacyjnych, charakteryzujących się bezwzględnym despektem wobec jakikolwiek granic politycznych, ekonomicznych czy administracyjnych.

Kilka lata temu, kiedy zaczęto stosować RODO, pojawiło się wiele mitów oraz obaw dotyczących realizacji przepisów w praktyce. Rozporządzenie, z uwagi na to że wprowadziło nowe instytucje prawne, które nominalnie miały przyczynić się do podniesienia poziomu ochrony danych osobowych, uległo swoistej fetyszyzacji zaburzając racjonalną ocenę wprowadzonych rozwiązań. W konsekwencji za niezwykle potrzebną należy uznać aposterioryczną (w stosunku do daty wejścia w życie przepisów) próbę wskazania niektórych wad i zalet nowego systemu GDPR. Na korzyść trzeba zaliczyć m.in.:

- próbę dopasowania zakresu wymagań do wielkości podmiotu (im większy podmiot, potencjalnie dysponujący większym spektrum danych, mogący wyrządzić więcej szkód na prywatności, tym większy zakres wymagań i odpowiedzialności),
- zagwarantowanie możliwości przetwarzania danych w ramach grup podmiotów (np. grup kapitałowych) w formule współadministrowania,
- powiązanie zakresu obowiązków ciążących na administratorze danych, w szczególności w obszarze zapewnienia bezpieczeństwa z procesem zarządzania ryzykiem, który powinien odbywać się w trybie ciągłym (w ramach koncepcji „*risk based approach*"),
- ustanowienie funkcji Inspektora Ochrony Danych, którego powołanie stało się co do zasady obowiązkowe lub zalecane, ze specyficznymi kompetencjami o charakterze wewnętrznego stanowiska nadzorczego, czuwającego nad prawidłowością realizacji procesów ODO w jednostce organizacyjnej, w której został powołany,
- poszerzenie katalogu praw osób, których dane dotyczą (których dane są przetwarzane), np. o prawo do bycia zapomnianym,
- modyfikację konstrukcji zgody na przetwarzanie z korzyścią dla osób, których dane są przetwarzane (wyeliminowanie zgód domyślnych),
- poszerzenie katalogu danych wrażliwych (sensytywnych), w szczególności o dane biometryczne, co poszerza krąg danych objętych podwyższonym poziomem ochrony,
- likwidację uciążliwego i dysfunkcjonalnego obowiązku rejestrowania w organie nadzorczym zbiorów danych,
- wprowadzenie wymogu uzyskania zgody na przetwarzanie danych osobowych dzieci, przez opiekunów prawnych,
- zwiększenie kontroli osoby, której dane dotyczą nad profilowaniem (automatycznym przetwarzaniem danych potrzebnych do analizy lub prognozy aspektów dotyczących

efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się),
- wprowadzenie nowych narzędzi ochrony danych (anonimizacji i pseudonimizacji),
- poszerzenie formuły kompleksowej współpracy ponadkrajowych organów nadzoru w ramach modelu „*OneStop-Shop*", i tym samym eliminacja zjawiska tzw. „forum shoppingu" (wybierania organu nadzoru w danym kraju przez korporacje działające w formie transnarodowej),
- wprowadzenie możliwości dyferencjacji oraz nakładania wyższych kar administracyjnych (w szczególności na globalnych potentatów przetwarzających dane na masową skalę) i w ślad za tym urealnienie kontroli nad gigantami usług cyfrowych,
- poszerzenie obowiązku informacyjnego, w szczególności wprowadzenie na masową skalę klauzul informacyjnych do domeny publicznej (szczególnie w Internecie),
- zastosowanie konieczności uzyskania zgód w relacji do celów przetwarzania, przy jednoczesnym zakazie uzyskiwania zgód łączonych, kompaktowych czy masowych (konieczność zaznaczania tzw. *check boxów*, odrębnie dla każdej zgody),
- wdrożenie obowiązku prowadzenia rejestru czynności związanych z przetwarzaniem danych (administratorzy danych) oraz rejestru kategorii czynności przetwarzania (procesorzy), co wymusiło lepszą identyfikację czynności i celów przetwarzania oraz wdrożenie odpowiednich środków bezpieczeństwa (technicznych i organizacyjnych),
- nałożenie konieczności dokonywania oceny skutków przetwarzania (*privacy impact assessment*) – już podczas projektowania systemu ochrony, w sytuacji gdy operacje przetwarzania stwarzają szczególne ryzyko dla praw i wolności podmiotów danych,
- zapewnienie procedury uprzedniej autentyfikacji indywidualnych systemów ochrony, oraz uprzednich konsultacji w zakresie procesów przetwarzania w ramach oceny skutków przetwarzania,
- wprowadzenie mechanizmów certyfikacji oraz znaków jakości i oznaczeń w zakresie ochrony danych osobowych, mających świadczyć o zgodności z rozporządzeniem operacji przetwarzania, prowadzonych przez administratorów i podmioty przetwarzające,
- sprywatyzowanie możliwości certyfikowania systemów ochrony danych osobowych,
- wprowadzenie możliwości publicznej rejestracji (potwierdzenia prawidłowości) dobrych praktyk, regulaminów, branżowych kodeksów postępowania z danymi osobowymi w ramach zrzeszeń, oraz akredytacji podmiotów monitorujących przestrzeganie,
- ułatwienie możliwości składania skarg do organów nadzorczych – w tym zapewnienie możliwości złożenia skargi bezpłatnie oraz do dowolnego organu nadzorczego, bez względu na lokalizacje państwową,
- zwiększenie praw osób, których dane dotyczą poprzez narzucenie obowiązku raportowania naruszeń bezpieczeństwa danych do organu nadzorczego bez zbędnej zwłoki, a jeżeli jest to wykonalne, nie później niż w czasie 72h po stwierdzeniu naruszenia,

- ustanowienie Europejskiej Rady Ochrony Danych, z kompetencjami w ramach mechanizmu spójności do wydawania wytycznych, opinii, rozstrzygania sporów pomiędzy organami nadzoru i wydawania wiążących decyzji.

Za generalną zaletę należy uznać przede wszystkim szeroko rozumiane konsekwencje, które stały się rezultatem medialnej kampanii, wstrząsu informacyjnego, jaki został wywołany wejściem w życie rozporządzenia. Odnotowano wzrost liczby publikacji nt. GDPR, wzrosła liczba opracowanych materiałów dziennikarskich, tekstów problemowych i poradników w zakresie stosowania RODO. W ślad za tym powstała chwilowa moda na dbanie o bezpieczeństwo danych osobowych. Opinia publiczna z dużą uwagą śledziła zwłaszcza informacje dotyczące administracyjnych kar pieniężnych. W konsekwencji spowodowało to, że niedostrzegana wcześniej sfera prawa, nie tyle ujrzała światło dzienne, co zawitała na pierwsze strony gazet. Nadto był to czas kształtowania odpowiednich postaw i swoistej edukacji społeczeństwa na temat ODO. Adresaci przepisów w dużej mierze po raz pierwszy dostrzegli konieczność podjęcia wysiłku zmierzającego do uporządkowania procesów gromadzenia, przetwarzania i ochrony danych osobowych w swoich organizacjach. Niezwykle popularne stało się porządkowanie dokumentacji dla tych wszystkich, którzy mieli ją nieaktualną lub w ogóle nie mieli. To pozytywy wynikające ze zmian.

Ocena natomiast może i powinna być relatywna albowiem to co miało stanowić zalety systemu, jednocześnie stało się jego obciążeniem. Tak ukształtowana warstwa normatywna nie ustrzegła się luk i deficytów. Z bardziej znaczących wad systemu można wskazać m.in.:

- wycofanie praktyki porządkowania procesów przetwarzania danych w oparciu o zbiory danych – co w przypadku niektórych administratorów danych (szczególnie małych i średnich) – skutkuje pewną dysfunkcjonalnością w zakresie identyfikacji procesów przetwarzania i przypisaniem do nich proporcjonalnego poziomu bezpieczeństwa,
- zniesienie poziomów bezpieczeństwa danych osobowych, które to poziomy pozwalały na korelację przedmiotowo-podmiotowa, tj. wielkości procesu przetwarzania danych osobowych u danego administratora do zakresu wdrażanych narzędzi bezpieczeństwa,
- brak precyzyjnej regulacji w zakresie udostępniania danych osobowych, co powoduje konieczność interpretacji sytuacji o charakterze udostępniania danych w oparciu o historyczne klisze prawne i praktykę, w szczególności na tle precyzyjnych przepisów regulujących kwestie powierzenia danych osobowych,
- jeszcze większe skomplikowanie systemu transferowania danych osobowych poza obszar EOG w sposób zgodny z prawem, co czyni go odrealnionym i w konsekwencji nieskutecznym, a przede wszystkich niestosowanym (zdecydowana większość wymiany danych do i spoza EOG odbywa się *de facto* poza ramami prawnymi przewidzianymi przez RODO i przepisy pokrewne),

- brak systemu wymiany danych poza obszar EOG skrojonego pod codzienne transfery niewielkich rozmiarów dokonywane przez użytkowników indywidulanych, (np. w zakresie korzystania z usług cyfrowych funkcjonujących w oparciu o sprzęt zlokalizowany poza granicami EOG, np. serwery),
- nieskuteczne narzucenie budowania ustawień domyślnych (*defaulty*), które również w dużej mierze nie spełniają swojego zadania z uwagi na to, że w większości są zaszyte w regulaminy, polityki, prywatności, umowy licencyjne, czy jakiekolwiek inne wielostronicowe kontrakty o charakterze adhezyjnym [z jednej strony ustawienia prywatności przygotowane przez zespół prawników i ekspertów technicznych opłacanych przez dostawców usług elektronicznych (*service providerów*), a z drugiej strony osoba fizyczna, która chcąc skorzystać z rozwiązania musi się zgodzić w całości na zaproponowaną treść umowy i na zaproponowane ustawienia prywatności],
- niezapobiegnięcie grzechowi pierworodnemu konstrukcji ustawień prywatności, który implikuje sytuacje, w której formalnie możne je zmienić, ale faktycznie, żeby móc cieszyć się funkcjonalnościami danej usługi czy urządzenia, i tak trzeba się na wszystko zgodzić, co dalej powoduje, że większość użytkowników odruchowo i bezrefleksyjnie akceptuje ustawienia zaproponowane przez usługodawcę – co zwrotnie unicestwia cel legislacyjny w postaci kontroli użytkowników nad ustawieniami prywatności,
- zlikwidowanie obowiązku posiadania dokumentacji systemu ochrony danych osobowych u administratora, w szczególności Polityki Bezpieczeństwa Danych Osobowych oraz Instrukcji Zarządzania Systemem Informacyjnym służącym do przetwarzania danych osobowych – co nadszarpnęło ugruntowaną praktykę porządkowania strukturę systemu, jego prowadzenia, uzupełniania, aktualizowania czy historycznego rejestrowania, w oparciu o tradycyjną dokumentację,
- anulacja funkcji Administratora Bezpieczeństwa Informacji przy jednoczesnym, narzuceniu zupełnie innej roli Inspektora Ochrony Danych z odmiennymi kompetencjami, w sytuacji gdy pozycja Administratora Bezpieczeństwa Informacji nie utraciła zasadności i jest nadal potrzebna w wewnętrznym systemie GDPR,
- wadliwe zaprojektowanie systemu odbierania zgód na przetwarzanie danych osobowych nieletnich przez opiekunów prawnych, co skutkuje fikcją w zakresie wykonywania nadzoru opiekunów prawnych nad procesami przetwarzania danych ich dzieci, z uwagi przede wszystkim na nieweryfikowalność podmiotu udzielającego zgody cyfrowo (na przetwarzającym dane spoczywa obowiązek dokonania weryfikacji wieku użytkownika oraz tego czy opiekun prawny dziecka udzielił zgody lub ją zaaprobował – czego nikt nie przestrzega),
- niewydolność systemu certyfikacji, uprzednich konsultacji oraz zatwierdzeń branżowych kodeksów postępowania przez organy nadzoru, wyrażająca się znikomym zainteresowaniem tymi instytucjami prawnymi,

- niedopracowanie obowiązku informacyjnego w nowej formie poprzez ustawienie klauzul informacyjnych w sposób, który w rzeczywistości stał się fikcją obowiązku informacyjnego albowiem – co prawda – stały się one powszechne, ale najczęściej są bardzo długie i uciążliwe w użytkowaniu, co z kolei powoduje że niewiele osób je czyta, zaś większość automatycznie zatwierdza (jest potrzeba urealnienia tego narzędzia, tak by nie było bezrefleksyjnym, szczególnie biorąc pod uwagę fakt, iż stanowi to każdorazowo oświadczenie woli w rozumieniu prawa cywilnego i administracyjnego,
- nieuniknięcie praktyki stosowania forteli pozwalających na ominięciu zakazu uzyskiwania zgód łączonych poprzez odpowiednie ustawienia tzw. *check boxów* dotyczących zgód na przetwarzanie danych, które co prawda muszą pozwalać na zaznaczanie zgód osobno – każdorazowo dla każdego z celów przetwarzania – faktycznie jednak narzucają szybsze zaznaczania kumulatywne,
- fatalny poziom ściągalności (egzekucji) nałożonych w formie pieniężnej kar administracyjnych.

Odpowiedzialność za naruszenia prawa ochrony danych osobowych – typologia

Zgodnie z postanowieniami rozporządzenia 2016/679 wyróżnia się dwa typy odpowiedzialności za prawidłowość przetwarzania danych osobowych:

1) odpowiedzialność za zgodność z prawem i prawidłowość procesów przetwarzania danych spoczywająca na: (a) administratorze danych, (b) współadministratorze, (c) podmiocie przetwarzającym (procesor *vel* processor) na podstawie powierzenia, podmiocie którym dane udostępniono oraz Inspektorze Danych Osobowych;
2) odpowiedzialność za nienaruszalność reguł wynikających z tych procesów, którą ponosi każdy kto uczestniczy w procesie przetwarzania danych osobowych.

Odpowiedzialność prawna może przybrać postać sankcji: (1) administracyjnych, (2) cywilnych, (3) karnych, (4) pracowniczych, (5) zawodowych, a także (6) korporacyjno-organizacyjnych. Niezależnie od powyższego w przypadku zbiegu naruszeń ochrony danych osobowych oraz szerzej chronionej prywatności, odpowiedzialność może się rozciągać chociażby o normy prawa cywilnego w zakresie ochrony prywatności jako dobra osobistego, czy międzynarodowe z racji ochrony prywatności jako podstawowych praw człowieka i obywatela. Stąd poszukując norm regulujących odpowiedzialność za niewystarczające należy uznać sięganie wyłącznie po przepisy wynikające z RODO.

Odpowiedzialność prawną podmiotu w sytuacji popełnienia deliktu ze sfery ochrony danych osobowych *ad casum* regulować mogą jednocześnie przepisy RODO, krajowej ustawy o ochronie danych osobowych, ustaw szczegółowych (np. w zakresu ochrony danych przetwarzanych w służbie zdrowia, chociażby odnoszących się do wymogów prowadzenia dokumentacji medycznej) czy ustaw generalnych, jak: kodeksu cywilnego (np. z zakresu ochrony dóbr osobistych), kodeksu postępowania administracyjnego (chociażby dot. postępowania przed Prezesem Urzędu ds. Ochrony Danych Osobowych), prawa o postępowaniu przed sądami administracyjnymi (w sytuacji odwołania się od decyzji urzędu nakładającej karę do sądu administracyjnego), kodeksu postępowania cywilnego, kodeksu karnego i kodeksu postępowania karnego (w przypadku podejrzenia popełnienia czynów zabronionych), kodeksu pracy (jeżeli delikt dotyczy sytuacji pracownika, bądź pracodawcy), rozporządzenia wykonawcze do w/w ustaw, normy etyki zawodowej, normy dyscyplinarne (w przypadku

samorządów zawodowych), czy wewnętrzne zasady korporacyjne, porządkowe i organizacyjne. Należy zatem podkreślić, że w ramach aktualnie obowiązujących regulacji, można mówić o złożonym systemie odpowiedzialności za naruszenie norm ochrony danych osobowych. Przy czym same RODO oraz ustawa o ochronie danych osobowych niewątpliwie zawierają normy specjalnie dedykowane wyłącznie tej przestrzeni sankcji prawnych.

Bez względu na rodzaj odpowiedzialności, pierwotnym źródłem naruszenia ochrony danych osobowych jest zawsze przetwarzanie bez uzasadnionej podstawy prawnej. Stąd każdorazowo odpowiedzialność musi być w pierwszej kolejności analizowana pod kątem podstawy prawnej (przesłanki legalizacyjnej) do przetwarzania danych osobowych. W świetle przepisów ustawy z 1997 roku administrator mógł legalnie przetwarzać dane osobowe jeżeli:

1) spełnił przynajmniej jeden z równoprawnych, autonomicznych warunków uprawniających do legalnego wykonywania operacji na danych – w odniesieniu do tzw. danych zwykłych (określonych w art. 23 ust 1 pkt 1–5[426]), w odniesieniu do danych szczególnie chronionych (określonych w art. 27 ust. 2 pkt 1–10[427]);
2) zastosował odpowiednie zabezpieczenia[428], w tym wdrożył środki techniczne i organizacyjne zabezpieczające dane przed ich udostępnieniem osobom nieupoważnionym, zebraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz utratą, uszkodzeniem lub zniszczeniem;
3) dopełnił obowiązków informacyjnych, w szczególności poinformował o swojej nazwie i adresie, celu zbierania, odbiorcach danych, prawie dostępu do danych i prawie ich poprawiania, a także o dobrowolności albo obowiązku podania danych – w przypadku zbierania danych bezpośrednio od osoby, której dane dotyczyły, natomiast w przypadku zbierania danych nie od osoby, której one dotyczyły poinformował o swojej nazwie i adresie, celu i zakresie zbierania danych, a zwłaszcza o ich odbiorcach, źródle, z którego

[426] Przetwarzanie danych osobowych „zwykłych" było dopuszczalne w sytuacji gdy: (1) osoba, której dane dotyczą, wyraziła na to zgodę, chyba że chodzi o usunięcie tych danych; (2) było to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa; (3) było to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą; (4) było niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego; (5) było to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą. Zob. art. 23 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 1997 nr 133 poz. 883 z późn. zm.).

[427] Przetwarzanie danych osobowych „wrażliwych" było jednak dopuszczalne, jeżeli: (1) osoba, której dane dotyczą, wyraziła na to zgodę na piśmie, chyba że chodziło o usunięcie dotyczących jej danych; (2) przepis szczególny innej ustawy zezwalał na przetwarzanie takich danych bez zgody osoby, której dane dotyczą, i stwarzał pełne gwarancje ich ochrony; (3) przetwarzanie takich danych było niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby, gdy osoba, której dane dotyczą, nie jest fizycznie lub prawnie zdolna do wyrażenia zgody, do czasu ustanowienia opiekuna prawnego lub kuratora; (4) było to niezbędne do wykonania statutowych zadań kościołów i innych związków wyznaniowych, stowarzyszeń, fundacji lub innych niezarobkowych organizacji lub instytucji o celach politycznych, naukowych, religijnych, filozoficznych lub związkowych, pod warunkiem, że przetwarzanie danych dotyczy wyłącznie członków tych organizacji lub instytucji albo osób utrzymujących z nimi stałe kontakty w związku z ich działalnością i zapewnione były pełne gwarancje ochrony przetwarzanych danych; (5) przetwarzanie dotyczy danych, które były niezbędne do dochodzenia praw przed sądem; (6) przetwarzanie było niezbędne do wykonania zadań administratora danych odnoszących się do zatrudnienia pracowników i innych osób, a zakres przetwarzanych danych był określony w ustawie; (7) przetwarzanie było prowadzone w celu ochrony stanu zdrowia, świadczenia usług medycznych lub leczenia pacjentów przez osoby trudniące się zawodowo leczeniem lub świadczeniem innych usług medycznych, zarządzania udzielaniem usług medycznych i były stworzone pełne gwarancje ochrony danych osobowych; (8) przetwarzanie dotyczy danych, które zostały podane do wiadomości publicznej przez osobę, której dane dotyczą; (9) było to niezbędne do prowadzenia badań naukowych, w tym do przygotowania rozprawy wymaganej do uzyskania dyplomu ukończenia szkoły wyższej lub stopnia naukowego, przy czym publikowanie wyników badań naukowych nie mogło następować w sposób umożliwiający identyfikację osób, których dane zostały przetworzone; (10) przetwarzanie danych było prowadzone przez stronę w celu realizacji praw i obowiązków wynikających z orzeczenia wydanego w postępowaniu sądowym lub administracyjnym. Zob. art. 27 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 1997 nr 133 poz. 883 z późn. zm.).

[428] Poziomy i zakres zabezpieczeń regulował rozdział 5 ustawy o ochronie danych osobowych oraz rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. z 2004r. Nr 100, poz. 1024).

dane pozyskał, prawie dostępu do danych i prawie ich poprawiania, a także o prawie żądania zaprzestania przetwarzania danych lub wniesienia sprzeciwu[429];

4) dołożył szczególnej staranności w celu ochrony interesów osób, których dane dotyczyły, poprzez zapewnienie, aby dane były przetwarzane zgodnie z prawem, dla oznaczonych celów, merytorycznie poprawne i adekwatne do celów, w jakich są przetwarzane, przechowywane w postaci umożliwiającej identyfikację osób, których dotyczyły, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania;
5) respektował prawa osób, których dane dotyczą – w szczególności te, dotyczące kontroli procesu przetwarzania danych;
6) dopełnił obowiązku rejestracji zbiorów danych w organie nadzorczym, w szczególności poprzez zgłoszenie do rejestru zbiorów prowadzonego przez organ administracyjny przed rozpoczęciem przetwarzania, z zastrzeżeniem relewantnych wyjątków[430];

Naruszenie przepisów o ochronie danych osobowych, w szczególności niedopełnienie obowiązków i warunków decydujących o tym, że przetwarzanie danych osobowych było legalne, mogło narazić administratora danych (względnie bezpośredniego sprawcę czynu zabronionego) na odpowiedzialność prawną. Z kolei, zgodnie z RODO, przetwarzanie jest legalne wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z poniższych warunków:

1) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
2) 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;

[429] W razie niedopełnienia przez administratora danych obowiązku uzupełnienia, uaktualnienia, sprostowania danych, czasowego lub stałego wstrzymania przetwarzania kwestionowanych danych lub ich usunięcia ze zbioru, osoba której dane dotyczą, mogła się zwrócić do administracyjnego organu nadzorczego z wnioskiem o nakazanie dopełnienia tego obowiązku. Zob. art. 32 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 1997 nr 133 poz. 883 z późn. zm.).

[430] Zgłoszeniu podlegały usystematyzowane dane, które były zbiorami w rozumieniu art. 7 pkt 1 ustawy, tj. były zbiorem o charakterze osobowym posiadającym strukturę, zestawionym według określonych kryteriów, niezależnie czy zbiór ten był rozproszony, zintegrowany, czy podzielony funkcjonalnie. Zwolnienia od zasady rejestracji zbiorów zostały określone w art. 43 ust. 1 ustawy. Jeżeli podmiot przetwarzał dane osobowe w zbiorze jako administrator danych, a jednocześnie nie zachodziła żadna z przesłanek derogacyjnych, to był on zobligowany do zgłoszenia tego zbioru do rejestracji. Z obowiązku rejestracji zbioru danych zwolnieni byli administratorzy danych zbiorów: (1) zawierających informacje niejawne, które zostały uzyskane w wyniku czynności operacyjno-rozpoznawczych przez funkcjonariuszy organów uprawnionych do tych czynności, (2) przetwarzanych przez właściwe organy dla potrzeb postępowania sądowego oraz na podstawie przepisów o Krajowym Rejestrze Karnym, (3) przetwarzanych przez Generalnego Inspektora Informacji Finansowej, (4) przetwarzanych przez właściwe organy na potrzeby udziału RP w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym, (5) dotyczących osób należących do kościoła lub innego związku wyznaniowego, o uregulowanej sytuacji prawnej, przetwarzanych na potrzeby tego kościoła lub związku wyznaniowego, (6) przetwarzanych w związku z zatrudnieniem u nich, świadczeniem im usług na podstawie umów cywilnoprawnych, a także dotyczących osób u nich zrzeszonych lub uczących się, (7) dotyczących osób korzystających z ich usług medycznych, obsługi notarialnej, adwokackiej, radcy prawnego, rzecznika patentowego, doradcy podatkowego lub biegłego rewidenta, (8) tworzonych na podstawie przepisów dotyczących wyborów do Sejmu, Senatu, Parlamentu Europejskiego, rad gmin, rad powiatów i sejmików województw, wyborów na urząd Prezydenta Rzeczypospolitej Polskiej, na wójta, burmistrza, prezydenta miasta oraz dotyczących referendum ogólnokrajowego i referendum lokalnego, (9) dotyczących osób pozbawionych wolności na podstawie ustawy, w zakresie niezbędnym do wykonania tymczasowego aresztowania lub kary pozbawienia wolności, (10) przetwarzanych wyłącznie w celu wystawienia faktury, rachunku lub prowadzenia sprawozdawczości finansowej, (11) powszechnie dostępnych, (12) przetwarzanych w celu przygotowania rozprawy wymaganej do uzyskania dyplomu ukończenia szkoły wyższej lub stopnia naukowego, (13) przetwarzanych w zakresie drobnych bieżących spraw życia codziennego, (14) które nie są prowadzone z wykorzystaniem systemów informatycznych, chyba że zawierają dane wrażliwe. Zgłoszenia zbioru do rejestracji należało dokonać przed rozpoczęciem przetwarzania danych, czyli przed pierwszą czynnością, jaką administrator może wykonać na danych. W sytuacji gdy administrator danych zamierzał przetwarzać tzw. dane szczególnie chronione, to zbieranie tego typu danych, mógł rozpocząć dopiero po zarejestrowaniu zbioru, chyba że ustawa zwalniała go z tego obowiązku. Od 1 stycznia 2015 roku, zgodnie z art. 43 ust. 1a znowelizowanej ustawy, z obowiązku rejestracji zbiorów danych osobowych (z wyjątkiem zbiorów zawierających dane wrażliwe) wyłączony był administrator danych, który powołał administratora bezpieczeństwa informacji i zgłosił fakt jego powołania do organu nadzorczego. W tej sytuacji zbiór podlegał rejestracji przy ABI, na którym ciążył obowiązek składania corocznych raportów z obsługi zbioru do organu nadzorczego. Zob. art. 43 ust. 1 i 1a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 1997 nr 133 poz. 883 z późn. zm.).

3) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
4) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
5) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
6) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią[431], 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 (akapit pierwszy lit. f) nie ma zastosowania do przetwarzania, którego dokonują organy publiczne w ramach realizacji swoich zadań)[432].

W przeciwieństwie do dyrektywy 95/46/WE konstrukcja prawna dopuszczalności przetwarzania sensytywnych danych osobowych w RODO nie jest oparta na wprowadzeniu podwyższonych wymogów przetwarzania wobec tej kategorii danych lecz na wyjątkach od generalnej zasady, wprowadzającej zakaz przetwarzania danych wrażliwych[433]. Przepisem art. 9 rozporządzenia *a contrario* legalizuje przetwarzania takich danych, jeżeli spełniony jest jeden z poniższych warunków:

1) osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, chyba że prawo Unii lub prawo państwa członkowskiego przewidują, iż osoba, której dane dotyczą, nie może uchylić zakazu przetwarzania;

[431] Zgodnie z wytycznymi Grupy Roboczej art 29 z 9 kwietnia 2014 roku (opinia 6/2014) zachowującymi jednak w znacznej części aktualność mimo zmiany stanu prawnego, interes musi być wystarczająco jasno wyrażony, tak aby pozwolić na przeprowadzenie testu równowagi względem interesów oraz praw podstawowych osoby, której dane dotyczą. Wymaga to aby interes był rzeczywisty, obecny i odpowiadał aktualnym działalnościom lub korzyściom, które są oczekiwane w bardzo bliskiej przyszłości. Innymi słowy, interes, który będzie zbyt ogólny lub spekulatywny, nie będzie wystarczający. Co istotne, interesy mogą również dotyczyć osoby trzeciej. Charakter interesu może być różny. Niektóre interesy mogą być istotne lub z korzyścią dla całego społeczeństwa. Jako najczęściej identyfikowane interesy wskazano m.in: (a) wykorzystanie prawa do wolności wypowiedzi lub informacji, w tym w mediach i sztuce, (b) konwencjonalny marketing bezpośredni oraz inne formy marketingu lub reklamy, (c) niezamówione informacje niehandlowe, włączając w to kampanie wyborcze lub zbieranie środków na cele charytatywne, (d) egzekucja roszczeń prawnych, włączając w to zbieranie długów poprzez procedury pozasądowe, (e) zapobieganie oszustwom, niewłaściwemu korzystaniu z usług lub praniu pieniędzy, (f) monitoring dla celów bezpieczeństwa, (g) systemu informowania o nieprawidłowościach, (h) bezpieczeństwo fizyczne, informatyczne oraz sieciowe. Zob. *Prawo Internetu*, red. Podrecki P., Warszawa 2007. Por. J. Kulesza, *Międzynarodowe prawo Internetu*, Poznań 2010. Por.. Wytyczne Grupy Roboczej art 29 z 9 kwietnia 2014 r. (opinia 6/2014). Por. P. Litwiński, *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, Wyd. C.H. Beck, Warszawa 2017, s. 305.

[432] 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 stanowiących w demokratycznym społeczeństwie niezbędny i proporcjonalny środek służący zagwarantowaniu celów, o których mowa w art. 23 ust. 1, administrator – aby ustalić, czy przetwarzanie w innym celu jest zgodne z celem, w którym dane osobowe zostały pierwotnie zebrane – bierze pod uwagę między innymi: (a) wszelkie związki między celami, w których zebrano dane osobowe, a celami zamierzonego dalszego przetwarzania; (b) kontekst, w którym zebrano dane osobowe, w szczególności relację między osobami, których dane dotyczą, a administratorem; (c) charakter danych osobowych, w szczególności czy przetwarzane są szczególne kategorie danych osobowych zgodnie z art. 9 lub dane osobowe dotyczące wyroków skazujących i naruszeń prawa zgodnie z art. 10; (d) ewentualne konsekwencje zamierzonego dalszego przetwarzania dla osób, których dane dotyczą; (e) istnienie odpowiednich zabezpieczeń, w tym ewentualnie szyfrowania lub pseudonimizacji. Zob. art. 6 pkt. 4 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 (Dz. Urz. UE L 119 z dn. 4.05.2016, s. 1–88).

[433] Dane sensytywne to dane osobowe ujawniające 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. Zob. art. 9 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 (Dz. Urz. UE L 119 z dn. 4.05.2016, s. 1–88).

2) przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii lub prawem państwa członkowskiego, lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą;
3) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody;
4) przetwarzania dokonuje się w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych, pod warunkiem że przetwarzanie dotyczy wyłącznie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami oraz że dane osobowe nie są ujawniane poza tym podmiotem bez zgody osób, których dane dotyczą;
5) przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą;
6) przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy;
7) 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;
8) przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego lub zgodnie z umową z pracownikiem służby zdrowia i z zastrzeżeniem warunków i zabezpieczeń[434];
9) przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki

[434] Dane osobowe mogą być przetwarzane do celów profilaktyki zdrowotnej jeżeli są przetwarzane przez – lub na odpowiedzialność – pracownika podlegającego obowiązkowi zachowania tajemnicy zawodowej na mocy prawa Unii lub prawa państwa członkowskiego, lub przepisów ustanowionych przez właściwe organy krajowe lub przez inną osobę również podlegającą obowiązkowi zachowania tajemnicy zawodowej na mocy prawa Unii lub prawa państwa członkowskiego, lub przepisów ustanowionych przez właściwe organy krajowe. Zob. art. 9 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 (Dz. Urz. UE L 119 z dn. 4.05.2016, s. 1–88).

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;

10) przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1, na podstawie prawa Unii lub prawa państwa członkowskiego, które 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.

Ogólne przepisy odnoszące się do odpowiedzialności i rodzajów sankcji reguluje Rozdział VIII RODO „Środki ochrony prawnej, odpowiedzialność i sankcje", przewidując:

- prawo do wniesienia skargi do organu nadzorczego (art. 77 RODO),
- prawo do skutecznego środka ochrony prawnej przed sądem przeciwko organowi nadzorczemu (art. 78 RODO),
- prawo do skutecznego środka ochrony prawnej przed sądem przeciwko administratorowi lub podmiotowi przetwarzającemu (art. 79 RODO),
- prawo do odszkodowania i odpowiedzialność (art. 82 RODO),
- ogólne warunki nakładania administracyjnych kar pieniężnych (art. 83 RODO),
- sankcje (art. 84 RODO).

Administrator danych, współadministrator, precesor – zakresy odpowiedzialności

Odpowiedzialność podmiotów decydujących o procesach przetwarzania danych w jednostkach organizacyjnych (administrator danych, współadministrator) za naruszenie zasad ochrony danych osobowych, przewidziana przepisami rozporządzenia 2016/679, ma charakter odpowiedzialności:

1) administracyjnoprawnej, która egzekwowana jest przez właściwe organy nadzoru,
2) cywilnoprawnej (postępowanie sądowe w sprawie o odszkodowanie inicjuje osoba, której dane dotyczą).

W niektórych sytuacjach skomplikowanych relacji gospodarczych i prawnych pomiędzy podmiotami, ustalenie charakteru, w którym występuje podmiot przetwarzający dane osobowe, może nastręczać istotnych trudności. Przykładowo podmiot może uważać się za administratora danych w sytuacji, w której nie posiada on podstaw prawnych ku temu, lub też, co jest częściej spotykane, podmiot chciałby występować w procesie wyłącznie w roli procesora, podczas gdy z okoliczności wynika, że powinien ponosić pełną odpowiedzialność związaną z administrowaniem danymi, które gromadzi. Przy czym administratorzy są również zobowiązani

wspierać Inspektorów Ochrony Danych w wykonywaniu ich zadań, zapewniając im odpowiednie zasoby i warunki organizacyjne. Tu należy wyeksponować, iż ilekroć jest mowa o administratorze danych – rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę decydującą o celach i środkach przetwarzania danych osobowych. Występowanie w roli administratora jest wynikiem analizy stanu faktycznego, a nie ogólnej uznaniowości.

Zasada odpowiedzialności podmiotów decydujących o celach przetwarzania co do zasady nie doznaje wyłomu, z zastrzeżeniem sytuacji, w których zachodzi: (a) współadministrowanie danymi, (b) udostępnienie danych, (c) powierzenie danych. Prawidłowe określenie podmiotów uczestniczących w procesie przetwarzania jest kluczowe dla identyfikacji uprawnień oraz obowiązków prawnych *ergo* zakwalifikowania poszczególnych podmiotów w ramach kategorii prawnych, wreszcie przypisania im odpowiedzialności prawnej.

Kwalifikowanie podmiotów do jednej z tych trzech kategorii tj. (1) administrator, (2) podmiot, któremu dane udostępniono, (3) czy też podmiot przetwarzający na podstawie powierzenia – ma charakter obiektywny i następuje w związku z konkretnym stanem faktycznym. W tym zakresie pomocną staje się opinia 1/2010 w sprawie pojęć „administrator danych" i „przetwarzający" z dnia 16 lutego 2010 roku wydana przez Grupę Roboczą art. 29, która identyfikuje elementy dyferencyjne[435], w tym m.in. sprawowanie realnej kontroli nad:

1) przetwarzanymi danymi wynikającej z wyraźnych kompetencji prawnych [dotyczy to sytuacji, gdy szczegółowe kryteria potrzebne do jego określenia wynikają wprost z obowiązujących przepisów prawa, trzeba bowiem zwrócić uwagę, iż samo RODO wskazuje, że przepisy w prawie UE lub prawie państwa członkowskiego, mogą wprost wyznaczać administratora danych, precyzować konkretne kryteria wyznaczenia administratora lub wskazywać sytuację, w której przepisy prawa nakładają na określony podmiot jedynie obowiązek przetwarzania danych osobowych (*vide* art. 4 pkt. 7 RODO)];
2) przetwarzanymi danymi wynikającej z dorozumianej kompetencji (z przesłanką tą możemy się spotkać w sytuacji, w której przepis prawa nie określa wprost roli podmiotu jako administratora ani nie wskazuje na obowiązek gromadzenia przez określony podmiot danych osobowych, niemniej rola podmiotu jako administratora może jednak wynikać wówczas z pewnej utrwalonej praktyki, np.: pracodawca w odniesieniu do danych dotyczących jego pracowników, wydawca w odniesieniu do danych dotyczących abonentów, stowarzyszenie w odniesieniu do danych dotyczących jego członków lub osób wspierających);
3) przetwarzaniem danych wynikającym z faktycznego wpływu (kryterium to odnosi się już bezpośrednio do oceny okoliczności danego przypadku, co wynika to z faktu, iż brak jest przepisów szczególnych regulujących kwestię administrowania danymi lub ich gromadzenia oraz nie wykształciła się żadna praktyka w tym zakresie. W większości takich przypadków analizę rozpoczyna się od oceny stosunków umownych zachodzących pomiędzy

[435] Opinia 1/2010 w sprawie pojęć „administrator danych" i „przetwarzający" 00264/10/PL WP 169 z dnia 16 lutego 2010 roku wydana przez Grupę Roboczą Art. 29.

podmiotami występującymi w procesie przetwarzania danych osobowych. Przydzielenie odpowiedniego statusu (administratora lub podmiot przetwarzający) winno być zawsze zweryfikowane z faktycznym poziomem kontroli nad przetwarzaniem danych sprawowanym przez te podmioty – co powinno mieć charakter wiążący przy określaniu administratora albowiem podmiotu, który nie ma prawnej ani faktycznej kontroli nad określaniem celu i sposobu przetwarzania danych osobowych, nie można uważać za administratora)[436].

Trudność w określeniu pozycji prawnej podmiotu względem procesów przetwarzania danych wynika oczywiście ze złożoności sytuacji społecznych. Im bardziej skomplikowane procesy interaktywnego, wielowymiarowego przetwarzania danych w czasie rzeczywistym, tym większa potrzeba dysponowania odpowiednimi narzędziami weryfikacji podmiotów. Porządek prawny pod rządami RODO stara się widzieć ten problem (prawnie niedostrzegany przez dyrektywę 95/46/WE), wprowadzając nieznane wcześniej rozwiązanie pozwalające na kształtowanie procesów przetwarzania danych osobowych przez więcej niż jednego administratora danych.

Współadministrowanie

Jeżeli co najmniej dwóch administratorów wspólnie ustala cele i sposoby przetwarzania, są oni współadministratorami. W drodze wspólnych uzgodnień współadministratorzy w przejrzysty sposób określają odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z rozporządzenia, 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 RODO, chyba że przypadające im obowiązki i ich zakres określa prawo Unii lub prawo państwa członkowskiego, któremu administratorzy ci podlegają. W uzgodnieniach można wskazać punkt kontaktowy dla osób, których dane dotyczą. Uzgodnienia pomiędzy współadministratorami winny należycie odzwierciedlać odpowiednie zakresy obowiązków współadministratorów oraz relacje pomiędzy nimi a podmiotami, których dane dotyczą. Zasadnicza treść uzgodnień jest udostępniana podmiotom, których dane dotyczą. Niezależnie od uzgodnień, osoba, której dane dotyczą, może wykonywać przysługujące jej prawa wynikające z rozporządzenia wobec każdego z administratorów.

Współadministratorzy w oparciu o odrębną (co do treści) umowę, opierając się na przepisie art. 26 RODO, mogą zawrzeć uzgodnienia dotyczące zakresu swojej odpowiedzialności wewnętrznej (pomiędzy tymi administratorami) związanej z wypełnianiem obowiązków na podstawie przepisów rozporządzenia. Co do zasady jednak w relacji zewnętrznej ich odpowiedzialność będzie rozkładać się solidarnie (i regresowo wobec siebie).

[436] *Powierzenie przetwarzania danych osobowych – czym dokładnie jest i kiedy je stosujemy?*, https://odo24.pl/blog-post.powierzenie-przetwarzania-danych-osobowych-czym-dokladnie-jest-i-kiedy-je-stosujemy, [dostęp: 05.11.2020].

Udostępnienie

Przekazywanie danych pomiędzy dwoma podmiotami może być również zakwalifikowane jako udostępnienie tych danych. Przepisy nie wprowadzają definicji udostępnienia danych osobowych. Niezależnie od powyższego pojęcie to jest powszechnie stosowane w praktyce. Poprzez udostępnienie danych należy rozumieć nic innego jak jedną z form przetwarzania danych osobowych, o czym stanowi sam art. 4 pkt. 2 RODO. Przepis wskazuje, że przetwarzanie oznacza operacje lub zestaw operacji na danych osobowych takich jak m.in. rozpowszechnianie lub innego rodzaju udostępnianie. Zgodnie z przyjętymi poglądami cechą charakterystyczną dla tej formy przetwarzania jest to, że dochodzi do niej w sytuacji, gdy dane przekazywane są pomiędzy dwoma podmiotami samodzielnie decydującymi o celach i środkach przetwarzania danych osobowych. Mając to na uwadze w tym przypadku odbiorcą danych będzie jedynie odrębny administrator. Należy zwrócić uwagę, że przy udostępnieniu danych, przepisy RODO nie przewidują szczególnych zasad realizacji udostępnienia, np. konieczność zawarcia stosownej umowy. Charakter czynności udostępnienia danych należy zatem oceniać jako czynność faktyczną, co oznacza, że może ono nastąpić w dowolny sposób skutkujący uzyskaniem przez odbiorcę dostępu do danych osobowych. Ważne jest umożliwienie rzeczywistego i samodzielnego podejmowanie decyzji odnośnie celów i sposobów przetwarzania danych. Nie można zatem mówić o udostępnieniu danych w relacji pomiędzy administratorem danych a podmiotem przetwarzającym w rozumieniu art. 4 pkt. 8 RODO, gdyż ten ostatni działa tylko i wyłącznie w zakresie celów i sposób określonych przez samego administratora.

Podobnie jak w przypadku współadministrowania to strony stosunku udostępnienia mogą, np. w oparciu o zawartą umowę, uzgodnić zakres swojej odpowiedzialności wewnętrznej związanej z wypełnianiem obowiązków na podstawie przepisów RODO. Ich odpowiedzialność będzie rozkładać się indywidualnie – w relacji do ich samodzielnych decyzji co do celu i środków przetwarzania danych. W relacji zewnętrznej odpowiedzialność będzie solidarna.

Powierzenie

Zasada, zgodnie z którą odpowiedzialność za przestrzeganie przepisów ochrony danych osobowych spoczywa na administratorze danych, zostaje uzupełniona – w przypadku instytucji powierzenia danych osobowych procesorowi – odpowiedzialnością administracyjną, cywilną, a nawet karną podmiotu, z którym została zawarta umowa powierzenia. Art. 4 pkt 8 RODO zawiera definicję samego podmiotu przetwarzającego (procesora), przez który należy rozumieć osobę fizyczną lub prawną, organ publicznym jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora.

Prawo zezwala administratorowi danych na powierzenie przetwarzania danych innemu podmiotowi na podstawie zawartej na piśmie umowy lub „innego instrumentu prawnego”[437].

[437] Przy tym należy podkreślić, że na administratorze danych ciąży obowiązek posiadania podstawy prawnej przetwarzania (czyli np. zgody podmiotu, którego dane osobowe przetwarza). Tym samym instytucja powierzenia przetwarzania danych osobowych podmiotowi trzeciemu polega m.in. na tym, iż nie jest wymagane uzyskanie zgody osoby, której dane dotyczą, na powierzenie jej danych. Powierzenie przetwarzania danych osobowych nie wymaga również

Powierzenie przetwarzania danych osobowych jest zleceniem wykonania czynności przetwarzania danych osobowych na rzecz administratora danych przez podmiot zewnętrzny (procesora), na podstawie stosownego postanowienia w umowie zapewniającego warunki bezpieczeństwa danych osobowych. Podmiot, który przyjmuje dane w powierzenie z związku z zawarta umową nie staje się ich administratorem, ponieważ nie decyduje o celach i środkach przetwarzania danych. Tym samym procesor nie jest administratorem danych osobowych, które mu powierzono – przetwarza je w imieniu, na rzecz i za zgodą zleceniodawcy, tj. administratora danych. Procesor nie może angażować się w proces przetwarzania powierzonych danych swoich podwykonawców, chyba że zostali oni uwzględnieni w umowie powierzenia przetwarzania danych lub została podpisana zgoda przez administratora na uwzględnienie podwykonawców (dalszych procesorów *vel* podprocesorów) w realizację zadań zleconych.

Przepisy rozporządzenia przewidują dwie kategorie obowiązków ciążących na procesorze w związku z przetwarzaniem powierzonych danych osobowych. Pierwsza kategoria obejmuje obowiązki, które powinny wynikać z umowy powierzenia zawartej z administratorem (art. 28 RODO). Postanowienia umowne dotyczące powierzenia przetwarzania danych osobowych można zawrzeć w umowie głównej bądź w formie aneksu do umowy głównej lub w postaci odrębnej umowy powierzenia. Umowa powierzenia przetwarzania danych osobowych powinna zawierać przede wszystkim zakres (katalog operacji wykonywanych na danych osobowych) i cel (przeznaczenie danych) przetwarzania danych. Nadto powinna regulować: charakter powierzenia, przedmiot, rodzaj danych, kategorię osób, których dane dotyczą, czas trwania powierzenia, obowiązki i prawa administratora, zgodę na podpowierzenia, zobligowanie osób upoważnionych do zachowania tajemnicy, stosowanie odpowiednich zabezpieczeń zgodnie z RODO, pomoc w realizacji praw osób, których dane są przetwarzane, pomoc administratorowi w wypełnianiu obowiązków notyfikacyjnych o naruszeniach względem UODO, usunięcie lub zwrot danych po ustaniu powierzenia, zgodę na poddanie się kontroli przeprowadzonej przez administratora.

Do drugiej kategorii wymogów nałożonych na procesora można zaliczyć samodzielne obowiązki, czyli wynikające bezpośrednio z przepisów powszechnie obowiązujących. Do zobowiązań, których źródłem są przepisy rozporządzenia będą należeć następujące obowiązki:

- wyznaczenie przedstawiciela w UE, jeśli jest to niezbędne (art. 27 RODO),
- niekorzystanie z usług innego podmiotu przetwarzającego bez zgody administratora (art. 28 ust. 2 RODO),
- przetwarzanie danych wyłącznie na polecenie administratora, przy czym podmiot przetwarzający niezwłocznie musi poinformować administratora, jeżeli jego zdaniem wydane mu polecenie stanowi naruszenie rozporządzenia lub innych przepisów Unii lub państwa członkowskiego o ochronie danych (art. 29 RODO),

informowania osób zainteresowanych o takiej czynności. Zob. A. Borowska, *Powierzenie danych osobowych – na czym polega?*, https://poradnikprzedsiebiorcy.pl/-na-czym-polega-powierzenie-danych-osobowych, [dostęp: 15.12.2020].

- prowadzenie rejestru kategorii czynności przetwarzania dokonywanych w imieniu administratora (art. 30 ust. 2 RODO),
- współpraca z organem nadzorczym (art. 31 RODO),
- niezwłoczne zgłoszenie administratorowi naruszenia ochrony danych osobowych (art. 33 ust. 2 RODO),
- powołanie Inspektora Ochrony Danych w sytuacji, w której zachodzi taki prawny obowiązek (art. 37 ust. 1 RODO).

Ponadto każdy podmiot przetwarzający dane (także procesor) prowadzi rejestr kategorii czynności przetwarzania dokonywanych w imieniu administratora, zawierający co najmniej takie informacje jak: (a) imię i nazwisko lub nazwę oraz dane kontaktowe podmiotu przetwarzającego lub podmiotów przetwarzających oraz każdego administratora, w imieniu którego działa podmiot przetwarzający, a gdy ma to zastosowanie – przedstawiciela administratora lub podmiotu przetwarzającego oraz Inspektora Ochrony Danych, (b) kategorie przetwarzań dokonywanych w imieniu każdego z administratorów, (c) przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, oraz gdy ma to zastosowanie – dokumentacja odpowiednich zabezpieczeń, (d) opis technicznych i organizacyjnych środków bezpieczeństwa.

Obowiązkiem procesora jest również podjęcie odpowiednich środków zabezpieczających przetwarzanie (art. 32 RODO), co oznacza m.in.:

- zapewnienie, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy,
- na zasadzie pomocy administratorowi stosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzania danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a także zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, oraz zmianą, utratą, uszkodzeniem lub zniszczeniem,
- na zasadzie pomocy administratorowi oceną skutków dla ochrony danych i uprzednimi konsultacjami (art. 32–36 RODO),
- dopuszczenie do przetwarzania danych jedynie osoby posiadające upoważnienie do przetwarzania danych osobowych, oraz prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych,
- pomoc administratorowi w wywiązywaniu się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw,
- udostępnianie administratorowi wszelkich informacji niezbędnych do wykazania spełnienia obowiązków wynikających z RODO oraz umożliwianie administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzenia audytów i kontroli,

- po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji administratora usunięcie lub zwrot wszelkich danych osobowych oraz usunięcie wszelkich ich istniejących kopii, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.

Co do zasady procesor odpowiedzialny jest w zakresie odpowiedzialności cywilnej – kontraktowej wobec administratora danych za niewykonanie lub nienależyte wykonanie umowy (art. 471 k.c.) oraz deliktowej (art. 415 k.c.). Natomiast wraz z administratorem danych na gruncie odpowiedzialności cywilnej wobec osoby, której dane dotyczą, procesor odpowiada na zasadach ogólnych, z tytułu naruszenia dóbr osobistych (art. 23 i 24 oraz 415 i 448 k.c.).

Z kolei sam administrator danych – w ramach zdarzeń wynikających z ustanowienia powierzenia – może ponosić odpowiedzialność na zasadzie ryzyka w przypadku bezprawnego działania procesora, działającego na jego zlecenie (art. 429 i 430 k.c.). Oczywiście administrator lub podmiot przetwarzający będą odpowiadać w przypadku wystąpienia łącznie następujących przesłanek:

1) poniesienia przez osobę, której dane dotyczą szkody (majątkowej lub niemajątkowej),
2) naruszenia przez administratora lub procesora przepisów RODO,
3) zaistnienia związku pomiędzy szkodą a naruszeniem,
4) wystąpienia winy.

Na procesorze (podobnie jak na innych podmiotach) ciąży również odpowiedzialność karna[438]. Do wejścia w życie RODO na podstawie przepisów rozdziału 8 ustawy z 1997 roku, natomiast od reformy systemu ochrony danych osobowych na podstawie art. 107 nowej ustawy o ochronie danych osobowych z 2018 roku. Zgodnie z treścią przepisu ustawy ten kto przetwarza dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do ich przetwarzania nie jest uprawniony, podlega grzywnie**,** karze ograniczenia wolności**,** karze pozbawienia wolności do lat dwóch, w przypadkach szczególnych kategorii danych osobowych, do lat trzech. Przepis karny adresowany jest również do procesora, który przetwarza dane osobowe bez podstawy prawnej to legalizującej (wiąże się to z naruszeniem art. 6 albo 9 RODO), lub przetwarza dane pozostając poza kręgiem podmiotów do tego upoważnionych, tj. w stosunku do przetwarzanych danych nie posiada statusu administratora, podmiotu przetwarzającego, dalszego podmiotu przetwarzającego lub nie dysponuje upoważnieniem do przetwarzania danych nadanym przez administratora.

Na gruncie kar administracyjnych należy zauważyć, że katalog potencjalnej odpowiedzialności procesora wynikający z RODO został znacznie rozszerzony w porównaniu do wcześniej obowiązujących uregulowań. Przepisy ustawy z 1997 roku wprowadzały zasadę, zgodnie z którą

[438] W tym zakresie procesor mógł odpowiadać za przetwarzanie danych bez podstawy prawnej (art. 49), ich udostępnienie osobie nieupoważnionej (art. 51), naruszenie obowiązku zabezpieczenia danych (art. 52) czy też udaremnienie lub utrudnienie kontroli (art. 54a). Zob. art. 49–54a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 1997 nr 133 poz. 883 z późn. zm.).

to administrator danych odpowiedzialny był za wszystkie elementy procesu przetwarzania danych, również za wszelkie operacje realizowane przez procesora, przy czym administrator nie mógł zwolnić się z tej odpowiedzialności, niezależnie od przyjętej treści umowy powierzenia. W związku z tym administrator danych odpowiedzialny był również w przypadku, gdy procesor przetwarzał dane niezgodnie z umową powierzenia[439]. Zgodnie z art. 31 ust. 3 ustawy z 1997 roku procesor był zobowiązany jeszcze przed rozpoczęciem przetwarzania danych jedynie do ich odpowiedniego zabezpieczenia (zgodnie z art. 36–39 ustawy) i posiadania stosownej dokumentacji (art. 39a ustawy). W przypadku naruszenia tych przepisów procesor ponosił odpowiedzialność jak administrator danych.

Kwestią dyskusyjną była odpowiedzialność procesora za działania, do którego nie miały zastosowania uprawnienia kontrolne GIODO. Jednakże jak stwierdził sąd administracyjny, w orzeczeniu z 2008 roku, działalność procesora może być przedmiotem postępowania kontrolnego prowadzonego przez GIODO, a procesor adresatem jego decyzji[440]. Po nowelizacji ustawy z 2004 roku uprawnienia GIODO dotyczyły wprost wszystkich podmiotów przetwarzających dane osobowe. Ustawodawca w art. 31 ust. 3 *in fine* ustawy z 1997 roku doprecyzował odpowiedzialność procesora w zakresie nieprzestrzegania przepisów dotyczących zabezpieczenia przetwarzania danych, stanowiąc że ponosi on odpowiedzialność jak administrator danych. Jednocześnie, zgodnie z art. 31 ust. 4 *in fine* ustawy, odpowiedzialność procesora nie została wyłączona w przypadku przetwarzania danych niezgodnie z zawartą umową. W obu przypadkach, zgodnie z art. 31 ust. 5 starej ustawy, podmiot przetwarzający dane osobowe podlegał w pełni zakresowi nadzoru sprawowanego przez GIODO i mógł być adresatem jego decyzji.

Od wejścia w życie RODO, podmiot przetwarzający odpowiada wyłącznie za szkody spowodowane niedopełnieniem przez niego obowiązków, które nakłada na niego rozporządzenie oraz za działania wbrew zgodnym z prawem instrukcjom administratora danych. Tym samym, o odpowiedzialności procesora możemy mówić w przypadkach gdy:

1) przepisy RODO nakładają na procesora obowiązki, których niewykonanie lub nienależyte wykonanie spowodowało szkodę,
2) procesor działa niezgodnie ze zgodnymi z prawem instrukcjami administratora,
3) procesor świadomie działa zgodnie z niezgodnymi z prawem instrukcjami administratora.

W zakresie, w jakim rozporządzenie nie reguluje odpowiedzialności podmiotu przetwarzającego, strony umowy powierzenia przetwarzania danych osobowych mogą uregulować odpowiedzialność dyskrecjonalnie według własnego uznania. W tym zakresie mogą one m.in. ustanowić kary umowne za zachowanie podmiotu przetwarzającego stojące w sprzeczności z postanowieniami zawartej umowy.

[439] Zob. wyrok NSA z 21 lutego 2000r. (II SA 1785/99).
[440] Zob. wyrok WSA w Warszawie z 19 sierpnia 2008 r. (II SA/Wa 605/08).

Zgodnie art. 83 ust. 4 rozporządzenia administracyjnej karze pieniężnej podlega naruszenie przez administratora i procesora m.in. obowiązków wynikających z art. 8, 11, 25–39 oraz 42, 43 RODO[441]. Przy czym przepis art. 83 ust. 4 nie ogranicza odpowiedzialności procesora (w ramach kar administracyjnych) jedynie do przypadków naruszenia przez niego obowiązków wynikających wprost z przepisów rozporządzenia, ale obejmuje także odpowiedzialność procesora za przetwarzanie danych bez podstawy wynikającej z zawartej w umowie powierzenia oraz za naruszenie umowy powierzenia w zakresie kształtowanym treścią RODO[442]. Zgodnie art. 28 ust. 10 RODO, w sytuacji gdy podmiot przetwarzający narusza przepisy rozporządzenia przy określaniu celów i sposobów przetwarzania, uznaje się go za administratora danych w odniesieniu do tego przetwarzania. Ogólne rozporządzenie o ochronie danych wskazuje także, iż podmiot przetwarzający, w sytuacji gdy skorzysta z usług innego podmiotu przetwarzającego (podpowierzenie), a ten nie wywiąże się ze spoczywających na nim obowiązku ochrony danych – nadal ponosi odpowiedzialność wobec administratora danych za wypełnienie obowiązków tego innego podmiotu przetwarzającego (czyli odpowiedzialność spoczywa na pierwotnym podmiocie przetwarzającym). Niemniej należy przyjąć, iż podmiot przetwarzający może zostać zwolniony z tej odpowiedzialności, jeżeli udowodni, że w żaden sposób nie ponosi winy za zdarzenie, które doprowadziło do powstania szkody.

Konstrukcję odpowiedzialności procesora uzupełnia przepis art. 82 rozporządzenia, który jednoznacznie wskazuję, iż każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia norm RODO, ma prawo uzyskać (m.in. od podmiotu przetwarzającego) odszkodowanie za poniesioną szkodę. Tak kategoryczne brzmienie przepisu pozwala określić zakres samodzielnej odpowiedzialności administracyjnej procesora.

Odpowiedzialność administracyjnoprawna

Najważniejszym i jednocześnie najbardziej dotkliwym rodzajem sankcji przewidzianych w RODO są administracyjne kary pieniężne, które stypizowane są w przepisie art. 83 rozporządzenia. Literalna wykładnia w/w normy nakazuje przyjąć, iż kary mogą być nakładane przez organ nadzorczy tj. w Polsce przez Prezesa Urzędu Ochrony Danych Osobowych bezpośrednio po stwierdzeniu naruszenia.

Ustawodawca europejski, ustanawiając administracyjne kary pieniężne za naruszenie przepisów o ochronie danych osobowych, zdecydował się na ujednolicenie zasad ich nakładania

[441] Zob. 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.

[442] Wątpliwości dotyczące zakresu odpowiedzialności administracyjnej procesora za naruszenie obowiązków, wskazanych w art. 28 ust. 3 RODO (wywodzonych z umowy zawieranej z administratorem), wynikają z faktu, że niektóre z obowiązków wskazanych w tym przepisie pokrywają się z bezpośrednimi obowiązkami procesora, wynikającymi z odrębnych regulacji, np. art. 29 RODO (art. 28 ust. 3 lit. a RODO), ale też art. 32 RODO (art. 28 ust. 3 lit. c RODO). Wobec tego można postawić pytanie, w jakim celu prawodawca unijny, umieścił te same obowiązki w odrębnych przepisach, tj. zarówno w art. 28 ust. 3 RODO określającym obligatoryjne elementy umowy powierzenia zawieranej z administratorem, jak i w innych przepisach określających wprost obowiązki procesora. W związku z tym pomimo przedstawionego brzmienia art. 83 ust. 4 RODO uzasadniona wydaje się argumentacja, że w zakresie obowiązków wymienionych w art. 28 ust. 3 RODO (które jednocześnie nie zostały powtórzone w przepisach odrębnych) procesor będzie ponosił wyłącznie odpowiedzialność umowną (naruszenie umowy w tym zakresie nie zawsze będzie prowadziło do naruszenia przepisów RODO). Źródłem tych obowiązków jest bowiem umowa powierzenia. Przykładowo naruszenie obowiązku pomocy administratorowi w wywiązywaniu się z praw podmiotów danych określonych w art. 28 ust. 3 lit. f RODO nie musi prowadzić do naruszenia obowiązku realizacji praw podmiotów danych przez administratora, jeżeli administrator będzie w stanie zrealizować obowiązki w tym zakresie bez pomocy procesora. M. Gumularz, P. Kozik, *Odpowiedzialność administracyjna przy powierzaniu*, http://www.abi-expert.pl/wydania/pazdziernikgrudzien-2017/art,1881,odpowiedzialnosc-administracyjna-przy-powierzaniu.html, [dostęp: 07.10.2020].

przez organy nadzorcze, co było naturalną konsekwencją ujednolicenia wymogów dotyczących ochrony danych osobowych na poziomie UE. Jednolite reguły w tym zakresie były niezbędne do tego, by zapewnić jednolity poziom przestrzegania przepisów i uniknąć zjawiska tzw. *forum shopping*, czyli przenoszenia działalności do państw, w których sankcje za naruszenie tych samych wymogów są niższe. Miało to służyć przede wszystkim wzmocnieniu i zharmonizowaniu sankcji administracyjnych oraz jest.

Jak podkreśla się w doktrynie, sankcje administracyjne mają nie tylko charakter represyjny, ale również prewencyjny. Sankcja ma bowiem stanowić dolegliwość dla sprawcy naruszenia, i to niezależnie od tego, czy i jakie skutki wywołało naruszenie. Skuteczność sankcji należy rozumieć zarówno jako miara osiągania celu, jakim jest z jednej strony przywrócenie stanu zgodności z prawem, jak również zapobieganie naruszeniom w przyszłości. Kara jest więc skuteczna jeśli spełnia swoje funkcje. Charakter prewencyjny kary ma charakter odstraszający, zapobiegający popełnianiu podobnych naruszeń w przyszłości. Kara ma być ponadto proporcjonalna do charakteru naruszenia[443].

Rozporządzenie wprowadza stosunkowo wysokie – w relacji do wcześniejszych –administracyjne kary pieniężne. Wysokość kary określana jest indywidualnie w stosunku do każdego przedsiębiorcy. Jednocześnie organy nadzorcze państw członkowskich mają zapewnić, by te kary były „w każdym indywidualnym przypadku skuteczne, proporcjonalne i odstraszające" (art. 83 ust. 1 RODO). Rozporządzenie określa wyłącznie górne limity kar pieniężnych, dzieląc je na dwie grupy ze względu na rodzaj naruszenia. I tak w zależności od naruszenia przewiduje dwa pułapy kar:

1) w wysokości do 10 000 000 euro, a w przypadku przedsiębiorstwa – w wysokości do 2% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego lub,
2) w wysokości do 20 000 000 euro, a w przypadku przedsiębiorstwa – w wysokości do 4% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego.

Pozostawienie organom administracji pewnej władzy dyskrecjonalnej (uznaniowości) w zakresie określania wysokości kar nie oznacza ich dowolności. Biorąc pod uwagę zarówno wysokość kar, jak i szeroko ujęte kryteria miarkowania należy dostrzec wolę normodawcy europejskiego, który chciał wyposażyć organy nadzorcze w instrument proporcjonalnego karania podmiotów dopuszczających się naruszeń na masową skalę (którym to instrumentem wcześniej nie dysponował), przy jednoczesnym zachowaniu względnej miary wobec zjawisk indywidualnych, czy w mikroskali[444].

Choć nie istnieje zatem prawem przewidziana procedura obliczania wysokości kary, to można przyjąć, że organ w pierwszym kroku ustala wysokość obrotu, następnie oblicza, ile wynosi – w zależności od rodzaju czynu – 2% lub 4% rocznego światowego obrotu. W kolejnym kroku

[443] Szerzej zob. T. Szewc, *Publicznoprawna ochrona informacji*, C.H. Beck, Warszawa 2007.
[444] Zob. 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.

porównuje tak ustaloną kwotę z kwotą – odpowiednio – 10 lub 20 mln euro, wreszcie wybiera wyższą z nich. W przypadku przedsiębiorców dochodzi bowiem do porównania wysokości kary obliczonej „kwotowo" z wysokością obliczoną „procentowo", przy czym górną granicą procentowego określenia wysokości kary jest – w zależności od czynu – 2% lub 4% rocznego światowego obrotu. Tak określona kwota dopiero stanowi podstawę do ustalenia ostatecznej wysokości kary, i to na tym etapie organ bierze pod uwagę kryteria z art. 83 ust. 2 RODO. Zgodnie z przepisem organ powinien wziąć pod uwagę następujące czynniki:

1) charakter, wagę i czas trwania naruszenia przy uwzględnieniu charakteru, zakresu lub celu danego przetwarzania, liczby poszkodowanych osób, których dane dotyczą, oraz rozmiaru poniesionej przez nie szkody;
2) umyślny lub nieumyślny charakter naruszenia;
3) działania podjęte przez administratora lub podmiot przetwarzający w celu zminimalizowania szkody poniesionej przez osoby, których dane dotyczą;
4) stopień odpowiedzialności administratora lub podmiotu przetwarzającego z uwzględnieniem środków technicznych i organizacyjnych wdrożonych przez nich na mocy art. 25 (wymóg uwzględniania ochrony danych w fazie projektowania oraz o wymóg domyślnej ochrony danych) i art. 32 (wdrożenie środków bezpieczeństwa odpowiednich do ryzyka);
5) wszelkie stosowne wcześniejsze naruszenia ze strony administratora lub podmiotu przetwarzającego;
6) stopień współpracy z organem nadzorczym w celu usunięcia naruszenia oraz złagodzenia jego ewentualnych negatywnych skutków;
7) kategorie danych osobowych, których dotyczyło naruszenie;
8) sposób, w jaki organ nadzorczy dowiedział się o naruszeniu, w szczególności czy i w jakim zakresie administrator lub podmiot przetwarzający zgłosili naruszenie;
9) jeżeli wobec administratora lub podmiotu przetwarzającego, których sprawa dotyczy, zostały wcześniej zastosowane w tej samej sprawie środki naprawcze, o których mowa w art. 58 ust. 2 RODO (ostrzeżenia, upomnienia, nakazy itp.) – przestrzeganie tych środków;
10) stosowanie zatwierdzonych kodeksów postępowania lub zatwierdzonych mechanizmów certyfikacji; oraz
11) 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[445].

[445] Należy mieć na uwadze, że kryteria nakładania kary i jej wysokości, o których mowa w art. 83 ust. 2 rozporządzenia można zaklasyfikować dwojako: jako działania zapobiegawcze, oraz jako działania, które powinny być podjęte już po stwierdzeniu naruszenia. Niezwykle istotne są działania zapobiegawcze mogące mieć wpływ zarówno na decyzję o karze, jak i jej wysokości. Należy do nich zaliczyć wdrożenie środków technicznych i organizacyjnych zastosowanych przez administratora lub podmiot przetwarzający na mocy art. 25 i 32 (pkt 4) oraz stosowanie kodeksów postępowania lub mechanizmów certyfikacji (pkt 10 powyżej). Natomiast już po stwierdzeniu naruszenia warto podjąć działania wymienione w pkt 3, 6, 8 oraz 9, tj. czynności mające na celu minimalizację wyrządzonej szkody. Zob. Wytyczne 4/2021 w sprawie kodeksów postępowania jako narzędzia do przekazywania danych – wersja do konsultacji publicznych, przyjęte 7 lipca 2021r., Europejska Rada Ochrony Danych. Por. A. Skibińska, *Jak prezes UODO nakłada administracyjne kary pieniężne?*, https://www.

Kara niższa będzie miała zastosowanie w przypadku naruszenia przepisów dotyczących obowiązku:

1) uzyskania zgody od opiekuna dziecka poniżej 16. roku życia w przypadku oferowania dziecku usług społeczeństwa informacyjnego (art. 8),
2) przetwarzania niewymagającego identyfikacji (art. 11),
3) stosowania mechanizmów *privacy by design* i *privacy by default* (art. 25),
4) regulowania relacji pomiędzy współadministratorami zgodnie z wytycznymi rozporządzenie (art. 26),
5) wyznaczenia przedstawiciela na terenie Unii (art. 27),
6) przestrzegania przez podmiot przetwarzający obowiązków nałożonych na niego w umowie z administratorem i przepisach, obowiązku odpowiedniego uregulowania relacji z podmiotem przetwarzającym (art. 28),
7) przetwarzania z upoważnienia administratora lub podmiotu przetwarzającego (art. 29),
8) rejestrowania czynności przetwarzania (art. 30),
9) współpracy z organem nadzorczym (art. 31),
10) wdrożenia odpowiednich środków technicznych i organizacyjnych (art. 32);
11) zgłoszenia naruszenia ochrony danych osobowych organowi nadzorczemu (art. 33);
12) zawiadomienia osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych (art. 34);
13) oceny skutków planowanych operacji przetwarzania dla ochrony danych (art. 35);
14) uprzednich konsultacji z organem nadzorczym, w przypadku gdyby dany rodzaj przetwarzania powodował wysokie ryzyko, co potwierdziła ocena skutków dla ochrony danych (art. 36);
15) wyznaczenia Inspektora Ochrony Danych oraz zapewnienia mu odpowiednich zasobów i gwarancji niezależności (art. 37);
16) nadania odpowiedniego statusu Inspektora Ochrony Danych (art. 38);
17) wypełniania zadań Inspektora Ochrony Danych (art. 39);
18) podmiotu certyfikującego (art. 42, 43);
19) podmiotu monitorującego przestrzegania kodeksu postępowania w zakresie jego naruszania przez administratora lub podmiot przetwarzający, w tym zawieszania lub wykluczania administratora i podmiotu przetwarzającego spośród stosujących kodeks (art. 41 ust. 4).

Kara wyższa będzie miała zastosowanie w przypadku naruszenia przepisów dotyczących: (1) podstawowych zasad przetwarzania, w tym warunków uzyskania zgody (art. 5, 6, 7, 9), (2) praw osób, których dane dotyczą m.in.: prawa dostępu do danych, prawa do sprostowania, prawa do bycia zapomnianym, prawa do ograniczenia przetwarzania, prawa do przenoszenia danych, prawa do wniesienia sprzeciwu, prawa do tego, by nie podlegać decyzji, która

politykabezpieczenstwa.pl/pl/a/jak-prezes-uodo-naklada-administracyjne-kary-pieniezne, [dostęp: 19.12.2020].

opera się wyłącznie na zautomatyzowanym przetwarzaniu w tym profilowaniu (art. 12), (3) zasad transferu danych osobowych do państw trzecich lub organizacji międzynarodowych (art. 44–49), (4) wszelkich obowiązków wynikających z prawa państwa członkowskiego przyjętego w związku z zapewnieniem wolności wypowiedzi i informacji, przetwarzaniem danych w kontekście zatrudnienia, przetwarzaniem danych w celach archiwalnych, naukowych, historycznych, statystycznych, przetwarzaniem danych przez kościoły i związki wyznaniowe (rozdział IX rozporządzenia), (5) nieprzestrzegania nakazu tymczasowego lub ostatecznego ograniczenia przetwarzania lub zawieszenia przepływu danych orzeczonego przez organ nadzorczy, (7) prawa organu nadzorczego dostępu do siedziby administratora lub podmiotu przetwarzającego.

Należy zauważyć, iż w sytuacji gdy administrator lub podmiot przetwarzający umyślnie lub niedbale narusza kilka postanowień rozporządzenia w odniesieniu do tego samego procesu przetwarzania danych, powstaje możliwość nałożenia kilku kar, jednak łączna suma nie może przekroczyć maksymalnych limitów. W przypadku kar za naruszenie przepisów rozporządzenia, ich maksymalna wysokość potencjalnych może budzić respekt. Oczywiście tak ustawiona górna poprzeczka ma na celu realizować funkcje „prewencyjne" i „odstraszające", przy czym nie można stracić z pola widzenia tego, iż kara nie może być wymierzona ponad miarę. Tym samym istotna staje się świadomość w jakim zakresie można faktycznie ponieść odpowiedzialność. Perspektywę tę można uzyskać chociażby poprzez analizę naruszeń przepisów w Europie.

Do wejścia w życie RODO tajemnicą poliszynela było „zaszywanie" kar za naruszenia standardów ochrony danych osobowych w karach za delikty popełnianie na przepisach ochrony konkurencji i konsumentów[446]. Przykłady kar nakładanych za praktyki antykonkurencyjne:

1) Google
   - w czerwcu 2017 roku gigant dostał ponad 2,42 mld euro kary za nadużywanie dominującej pozycji swojej wyszukiwarki internetowej do niezgodnego z prawem preferencyjnego traktowania własnej porównywarki cenowej[447],
   - w lipcu 2018 roku Komisja Europejska nałożyła 4,3 mld euro kary za wymuszanie na producentach instalacji programów firmy w zamian za dostęp do sklepu z aplikacjami i darmowe wykorzystanie systemu Android (wymuszanie domyślnego ustawienia w komórkach wyszukiwarki Google i przeglądarki Chrome)[448],
   - w marcu 2019 roku Komisja Europejska nałożyła na Google 1,49 mld euro grzywny za uniemożliwianie konkurentom zamieszczania reklam na stronach, z którymi potentat

[446] Europejska polityka antymonopolowa opiera się na dwóch głównych zasadach określonych w Traktacie o funkcjonowaniu Unii Europejskiej Po pierwsze art. 101 Traktatu zakazuje porozumień między dwoma niezależnymi podmiotami gospodarczymi lub większą ich liczbą, które ograniczają konkurencję. Przepis ten obejmuje zarówno porozumienia horyzontalne (między faktycznymi lub potencjalnymi konkurentami działającymi na tym samym poziomie łańcucha dostaw), jak i porozumienia wertykalne (między przedsiębiorstwami działającymi na różnych poziomach, np. porozumienie między producentem a jego dystrybutorem). Po drugie art. 102 Traktatu zakazuje przedsiębiorstwom zajmującym pozycję dominującą na danym rynku nadużywania tej pozycji, na przykład poprzez stosowanie nieuczciwych cen, ograniczanie produkcji lub odmowę wprowadzania innowacji ze szkodą dla konsumentów. Szerzej zob. A. Maziarz, *Reguły konkurencji Unii Europejskiej*, C.H. Beck, Warszawa 2019.

[447] *Kara dla Google'a*, https://ec.europa.eu/poland/news/190320_google_pl, , [dostęp: 30.12.2020].

[448] *Rekordowa kara dla Google. Komisja Europejska nakazuje zapłacić aż 4,3 mld euro*, https://www.money.pl/gospodarka/unia-europejska/wiadomosci/artykul/kara-dla-google-komisja-europejska-android,85,0,2411349.html, [dostęp: 30.12.2020].

na rynku wyszukiwarek miał podpisane umowy (uniemożliwiały one konkurentom zamieszczanie reklam w wynikach wyszukiwania)[449],

- w czerwcu 2021 roku francuski urząd antymonopolowy (Autorité de la Concurrence) zobowiązał koncern Google (Alphabet) do zmiany praktyk na rynku reklamy internetowej, jednocześnie nakładając 220 mln euro kary[450];

2) Facebook

- w czerwcu 2021 roku Komisja Europejska wszczęła formalne dochodzenie antymonopolowe, które ma sprawdzić, czy największy portal społecznościowy na świecie naruszył unijne zasady konkurencji[451],
- w październiku 2021 roku Facebook został ukarany grzywną w wysokości 50,5 miliona funtów (69 milionów dolarów) za naruszenie nakazu nałożonego przez brytyjskiego regulatora konkurencji, przy przejęciu platformy do udostępniania gifów Giphy[452];

3) Microsoft

- w lutym 2008 roku Microsoft objęto karą w wysokości 899 mln euro za niedostosowanie się do decyzji Komisji Europejskiej z marca 2004 roku, kiedy to Komisja uznała, że Microsoft naliczał nieracjonalne ceny za dostęp do dokumentacji interfejsu dla serwerów grup roboczych [w decyzji z 2004 r., podtrzymanej przez Sąd Pierwszej Instancji we wrześniu 2007 r. (wyroki TS/07/63 i MEMO/07/359)] stwierdzono, że Microsoft nadużył pozycji dominującej na mocy art. 82 Traktatu WE, żądając ujawnienia dokumentacji interfejsów, która umożliwiłaby innym serwerom grup roboczych niż z Microsoft, osiągnięcie interoperacyjności z komputerami i serwerami z systemem Windows[453],
- w 2009 roku Komisja Europejska zamknęła toczącą się przeciwko Microsoftowi sprawę dotyczącą nieuczciwej konkurencji na rynku przeglądarek internetowych, przy czym koncern został zobowiązany do umożliwienia użytkownikom systemu operacyjnego Windows wyboru dowolnej przeglądarki internetowej (zamiast domyślnie oferować swój produkt – Internet Explorer)[454],
- w marcu 2013 roku Komisja Europejska, nałożyła na koncern Microsoft karę w wysokości 561 mln euro, za złamanie zobowiązania do zapewnienia użytkownikom systemu Windows możliwości łatwego wyboru przeglądarki internetowej (według KE przez 14 miesięcy – od maja 2011 r. do lipca 2012 r. – 15 milionów użytkowników systemu Windows 7 Service Pack 1 nie miało takiej możliwości)[455];

[449] *Kolejna miliardowa kara dla Google od Unii*, https://www.prawo.pl/biznes/google-ukarany-przez-ke-za-blokowanie-dostepu-konkurentom-do,389010.html, [dostęp: 30.12.2020].

[450] Zob. A. Wolska, *Francja: Google ukarany za działania w sferze reklamowej. Zapłaci 220 mln euro grzywny*, https://www.euractiv.pl/section/gospodarka/news/francja-google-ukarany-za-dzialania-w-sferze-reklamowej-zaplaci-220-mln-euro-grzywny/, [dostęp: 30.12.2020].

[451] *Unia Europejska grilluje Facebooka. Nasze dane mogły być wykorzystywane do nieuczciwej konkurencji*, https://www.money.pl/gospodarka/unia-europejska-grilluje-facebooka-ke-wszczyna-sledztwo-6648040035318432a.html, [dostęp: 30.12.2020].

[452] Zob. *Kara dla Facebooka. „Ostrzeżenie dla każdej firmy, która uważa, że jest ponad prawem"*, https://www.money.pl/gospodarka/potezna-kara-dla-facebooka-ostrzezenie-dla-kazdej-firmy-ktora-uwaza-ze-jest-ponad-prawem-6695940596378208a.html, [dostęp: 30.12.2020].

[453] A. Turek, *Google to nie wszystko. Największe kary antymonopolowe dla technologicznych gigantów w historii UE*, https://businessinsider.com.pl/firmy/zarzadzanie/kary-antymonopolowe-od-komisji-europejskiej-google-to-nie-wszystko/6z9216z, [dostęp: 30.12.2020].

[454] M. Kulesza, *Surowa kara dla Microsoftu*, https://codozasady.pl/p/surowa-kara-dla-microsoftu, [dostęp: 30.12.2020].

[455] *UE nałożyła na Microsoft 561 mln euro kary. Za przeglądarkę*, https://www.forbes.pl/technologie/ue-nalozyla-na-microsoft-561-mln-euro-kary-za-

4) Apple
   - w marcu 2020 roku francuski organ ochrony konkurencji nałożył na Apple karę w wysokości 1,1 miliarda euro (1,2 mld USD) kary za praktyki antykonkurencyjne polegające na zawieraniu nielegalnych porozumień w ramach sieci dystrybucyjnej i nadużywanie „zależności ekonomicznej" niezależnych sprzedawców (organ nałożył osobne grzywny na dwóch hurtowników Apple: Ingram Micro 76,1 mln EUR (85 mln USD) i Tech Data 62,9 mln EUR (70,3 mln USD), za współudział w naruszeniu prawa antymonopolowego[456],
   - w czerwcu 2020 roku Komisja Europejska rozpoczęła postępowanie antymonopolowe, by ocenić czy reguły Apple dotyczące dystrybucji aplikacji za pośrednictwem App Store naruszają unijne reguły konkurencji, przy czym KE równolegle wszczęła drugie postępowanie antymonopolowe wobec Apple mające sprawdzić czy aplikacja Apple Pay narusza unijne reguły konkurencji (dochodzenie dotyczy m.in. sposobów integracji Apple Pay z aplikacjami handlowymi i stronami internetowymi)[457],
   - w kwietniu 2021 roku Komisja Europejska pod groźbą nałożenia kary w wysokości 27 mld USD zobowiązała koncern do przesłania w terminie 12 tygodni stosownego wyjaśnienie w związku z ograniczeniami jakie nakładane są na aplikacje w sklepie AppStore (chodzi o ofertę Spotify, oraz wymóg korzystania z wewnętrznego systemu rozliczeniowego Apple)[458].
5) Intel
   - w 2009 roku koncern otrzymał od Komisji Europejskie 1,06 mld euro kary za niezgodne z prawem praktyki monopolowe mające na celu wykluczenie konkurentów z rynku procesorów komputerowych x86 (Komisja ustaliła, że Intel uczestniczył w dwóch konkretnych formach nielegalnych praktyk. Po pierwsze, Intel udzielał całkowicie lub częściowo ukrytych rabatów producentom komputerów pod warunkiem, że kupili oni wszystkie lub prawie wszystkie swoje procesory x86 od Intela. Po drugie, Intel dokonywał bezpośrednich płatności na rzecz producentów komputerów w celu wstrzymania lub opóźnienia wprowadzenia na rynek określonych produktów zawierających procesory x86 konkurencji oraz w celu ograniczenia kanałów sprzedaży dostępnych dla tych produktów)[459].

Z kolei na gruncie systemu ODO, jeszcze na podstawie „starych" przepisów o ochronie danych osobowych, sprzed RODO, krajowe organy ochrony danych osobowych państw członkowskich nakładały znaczące kary. Za najbardziej spektakularną należy uznać karę nałożona przez hiszpański organ ds. ochrony danych osobowych (agencja AEPD) na Facebook we wrześniu 2017 roku. Agencja uznała, iż firma przechowywała i wykorzystywała dane,

przegladarke/xeyd882, [dostęp: 30.12.2020].

[456] *Apple ma zapłacić 1,2 mld USD kary za praktyki antykonkurencyjne*, https://ithardware.pl/aktualnosci/apple_ma_zaplacic_1_2_mld_usd_kary_za_praktyki_antykonkurencyjne-11716.html, [dostęp: 30.07.2021].

[457] Dotyczyło to w szczególności obowiązkowego korzystania z zastrzeżonego przez Apple systemu zakupów oraz ograniczeń dotyczących możliwości informowania przez twórców aplikacji użytkowników iPhone'a i iPada o alternatywnych tańszych możliwościach zakupu. Zob. *KE wszczęła postepowania antymonopolowe wobec firmy Apple*, https://www.pb.pl/ke-wszczela-postepowania-antymonopolowe-wobec-firmy-apple-993943, [dostęp: 30.12.2020]

[458] *Apple oskarżone przez EU, grozi im kara w wysokości 27 mld USD*, https://antyweb.pl/apple-oskarzone-przez-eu-grozi-im-kara-w-wysokosci-27-mld-usd, [dostęp: 30.07.2021].

[459] *Google to nie wszystko. Największe kary antymonopolowe dla technologicznych gigantów w historii UE*, https://businessinsider.com.pl/firmy/zarzadzanie/kary-antymonopolowe-od-komisji-europejskiej-google-to-nie-wszystko/6z9216z, [dostęp: 30.12.2020]

w tym szczególnie chronione dane, do celów reklamowych bez uzyskania właściwej zgody i nałożyła na giganta karę w wysokości 1,2 mld euro[460].

W maju 2017 roku Komisja Europejska nałożyła 110 mln euro kary na Facebooka za podanie nieprawdziwych lub wprowadzających w błąd informacji podczas prowadzonego przez Komisję w 2014 r. dochodzenia w sprawie przejęcia WhatsApp przez Facebook na podstawie unijnego rozporządzenia w sprawie kontroli łączenia przedsiębiorstw. W toku procedury zatwierdzającej przejęcie, Facebook dostarczył organom unijnym nieprecyzyjnych danych o możliwości połączenia kont użytkowników serwisów Faceebook i WhatsApp. Informację, że numer telefonu użytkownika komunikatora można połączyć z profilem na portalu społecznościowym, Facebook ogłosił publicznie dopiero w sierpniu 2016 roku.

Najgłośniejszą sprawą związaną z naruszeniem prawa ochrony danych osobowych był międzynarodowy skandal wokół grupy Cambridge Analytica. Firma pozyskiwała z Facebooka informacje o 87 mln użytkowników tego serwisu, a następnie wykorzystała zgromadzone z naruszeniem prawa dane do celów marketingu politycznego[461]. Pod koniec 2018 roku brytyjski organ ochrony danych osobowych nałożył na Facebooka karę w wysokości 500 tys. funtów (644 tys. dolarów) za przekazywanie Brytyjczykom nieprawdziwych lub wprowadzających w błąd informacji dotyczących prywatności ich danych personalnych gromadzonych na Facebooku oraz Messengerze. Kara została orzeczona przez Information Commissioner's Office (ICO – Biuro Komisarza ds. Informacji). Owe 500 tys. funtów stanowiło maksymalny wymiar kary, jaki można było nałożyć na dany podmiot naruszający prawo ochrony danych osobowych przed wdrożeniem RODO[462].

Z kolei 2 lutego 2017 r. włoski organ ochrony danych (Garante) nałożył rekordową grzywnę w wysokości 5,880 mln euro na brytyjską spółkę działającą we Włoszech za naruszenie przepisów dotyczących konieczności uzyskania zgody na przetwarzanie danych[463].

---

[460] Agencja w uzasadnieniu wskazała, że dane dotyczące ideologii, płci, przekonań religijnych, osobistych preferencji lub czynności związanych z przeglądaniem są gromadzone bezpośrednio poprzez interakcję z ich usługami lub ze stron osób trzecich bez wyraźnego poinformowania użytkownika o tym, w jaki sposób i w jakim celu będą wykorzystywać te dane. Ponadto Facebook nie uzyskuje jednoznacznej, konkretnej i świadomej zgody użytkowników na przetwarzanie swoich danych, ponieważ informacje, które przekazuje, nie są pełne i właściwe. Dane użytkowników nie są całkowicie usuwane, gdy przestają być przydatne do celów, dla których zostały zebrane, ani gdy użytkownik wyraźnie zażąda ich usunięcia. Zob. R. Malujda, *Kary za naruszenie przepisów o ochronie danych osobowych*, https://malujda.pl/kary-za-naruszenie-przepisow-o-ochronie-danych-osobowych-ochrona-danych-osobowych/, [dostęp: 30.12.2020].

[461] Pozornie prosta aplikacja do testów osobowości zbierała dane nie tylko biorących w niej udział użytkowników, ale także ich znajomych, którzy nie wyrazili na to zgody. Choć udział w teście wzięło jedynie nieco ponad 300 tys. osób, aplikacja pobrała dane 87 mln osób. Informacje te potem zostały przynajmniej w części wykorzystane przez firmę Cambridge Analytica do targetowania politycznego i wyborczej rywalizacji. Afera Cambridge Analytica była punktem zwrotnym w ocenach Facebooka. Po jej ujawnieniu ludzie i media zaczęły znacznie mniej przychylnie patrzeć na portal. Opinia publiczna dowiedziała się jak przedmiotowo traktowani są użytkownicy oraz jak naruszana jest ich prywatność. Szerzej zob. G. Rydlewski, *Rządzenie w epoce informacji, cyfryzacji i sztucznej* inteligencji, Elipsa Dom Wydawniczy, Warszawa 2021.

[462] Zob. *Facebook zapłaci wysoką karę za skandal Cambridge Analytica*, https://www.komputerswiat.pl/aktualnosci/inne/facebook-zaplaci-wysoka-kare-za-skandal-cambridge-analytica/2s35j21, [dostęp: 30.12.2020]. Wcześniej Kanadyjskie Biuro ds. Konkurencji, stawiając te same zarzuty, zarzuciło portalowi, że od sierpnia 2012 r. do czerwca 2018 r. naruszał prywatność użytkowników i nałożyło karę w wysokości 6,5 mln dolarów. Por. *Facebook zapłaci karę za aferę Cambridge Analytica*, https://businessinsider.com.pl/wiadomosci/kara-dla-facebooka-za-afere-cambridge-analytica/9e6yzdd, [dostęp: 30.12.2020].

[463] Dokładną analizę procedowania włoskiego organu przeprowadził Rafał Malujda, który wskazuje, że według władz włoskich przedsiębiorstwa podzieliły duże transfery pieniężne na mniejsze w celu uniknięcia wykrycia, a następnie przypisały transfery podmiotom danych, które nie były tego świadome. Dane osobowe tych osób uzyskano z bazy danych utworzonej przez jedną z firm. Miało to nastąpić w celu ominięcia obowiązujących włoskich przepisów dotyczących przeciwdziałania praniu pieniędzy i uniknięcia ujawnienia nazw prawdziwych stron przekazujących pieniądze. Włoski regulator stwierdził, że firmy naruszyły zasady dotyczące prywatności, ponieważ przetwarzały dane osób bez ich wiedzy i zgody. Ponadto podniósł, że naruszenia zostały popełnione w związku z bazą danych o znacznym rozmiarze i znaczeniu. Garante nałożył wysokie kary na każdą z firm uczestniczących w systemie przekazów pieniężnych w wysokości odpowiednio: 5 880 000 euro, 1 590 000 euro, 1 430 000 euro, 1 260 000 euro i 850 000 euro, co dało łącznie ponad 11 milionów euro. Garante obliczył grzywny w następujący sposób: zastosował karę w wysokości 10 000 euro za każdy podmiot danych, którego prawa zostały naruszone, oraz zastosował dodatkową grzywnę w wysokości 50 000 euro ze względu na rozmiar i znaczenie bazy danych. Przetwarzanie obejmowało 583 podmiotów danych bez ich zgody. Garante nałożył zatem grzywnę w wysokości 5 880 000 euro (10 000 euro pomnożoną przez 583 ofiary plus kolejne 50 000 euro). Zob. R. Malujda, *Kary za naruszenie przepisów o ochronie danych osobowych*, https://malujda.pl/kary-za-naruszenie-przepisow-o-ochronie-danych-osobowych-ochrona-danych-osobowych/, [dostęp: 30.12.2020].

W tym samym roku Holenderski Urząd Ochrony Danych (DPA) po przeprowadzeniu dochodzenia w sprawie Windows 10 Home i Pro stwierdził, iż Microsoft naruszył prawo ochrony danych w ramach systemie Windows 10. Organ stwierdził ponadto, że Microsoft nie mógł przetwarzać danych w tym zakresie na podstawie zgody użytkownika – nie była ona bowiem jednoznaczna i nie zawierała wymaganej warstwy informacyjnej[464]. Holandia stała się ówcześnie drugim państwem w Unii Europejskiej, gdzie stwierdzono, że Windows 10 narusza prawo w zakresie danych osobowych. Wcześniej podobna sytuacja miała miejsce we Francji, gdzie na skutek interwencji tamtejszych organów Microsoft poprawił ustawienia w zakresie prywatności (zmiany pojawiły się głównie w Creators Update)[465].

Na chwilę przed wejściem w życie RODO, jeszcze w sierpniu 2018 roku francuska firma Optical Partners została ukarana na kwotę 250 tysięcy euro za udostępnienie ponad 300 tysięcy dokumentów zawierających wrażliwe informacje o klientach. Z kolei karą w wysokości 500 tys. funtów objęto brytyjską firmę Equifax, która nie zastosowała odpowiedniej technologii do ochrony danych 150 mln klientów[466].

Już pod rządami RODO przykłady kar nakładanych na gigantów teleinformatycznych za naruszenia standardów ochrony danych osobowych obejmują m.in. następujące przypadki.

21 stycznia 2019 roku koncern Google został obciążony karą 57 milionów euro nałożoną przez francuski organ ochrony danych CNIL (Commission Nationale de L'informatique et des Libertés), który uznał, że firma nie informowała użytkowników przejrzyście i nie uzyskiwała zgód w odpowiedni sposób. Informacje o przetwarzaniu danych rozłożono na różne dokumenty i użytkownik nie mógł łatwo ustalić np. czasu przetwarzania danych lub kategorii danych użytych do personalizacji. Nadto cele przetwarzania danych opisano w sposób zbyt ogólny i niejasny. Poza tym CNIL miał zastrzeżenia co do ważności zgód uzyskiwanych przez Google, w szczególności udzielone zgody nie były jednoznaczne, a same zgody były zbierane „hurtowo" na warunki Google i Politykę Prywatności, podczas gdy przepisy wymagają osobnej zgody dla każdego celu przetwarzania[467].

15 lipca 2019 roku amerykańska Federalna Komisja Handlu (FTC), w wyniku zwartej ugody, ukarała koncern grzywną w wysokości 5 mld dolarów za ograniczenia możliwości wyborów konsumenckich. Treść porozumienia przewidywała również, że Facebook będzie musiał stworzyć specjalny komitet nadzorujący to jak spółka wykorzystuje dane osobowe. Tłem dla tej ugody była afera związana z firmą Cambridge Analytica[468].

---

[464] Firma Microsoft nie informowała bowiem użytkownika w jasny sposób o typie danych, których używa i do jakiego celu. Ponadto użytkownicy nie mogli udzielić prawidłowej zgody na przetwarzanie swoich danych osobowych. Firma nie informowała użytkowników jednoznacznie o ciągłym gromadzeniu danych osobowych w zakresie korzystania z aplikacji i zachowań związanych z przeglądaniem stron internetowych za pośrednictwem przeglądarki Edge, gdy używane są ustawienia domyślne. Zob. R. Malujda, *Kary za naruszenie przepisów o ochronie danych osobowych*, https://malujda.pl/kary-za-naruszenie-przepisow-o-ochronie-danych-osobowych-ochrona-danych-osobowych/, [dostęp: 30.12.2020].

[465] Szerzej zob. A. Bała, *Holandia: Zbieranie danych przez Windows 10 nielegalne*, https://www.purepc.pl/holandia-zbieranie-danych-przez-windows-10-nielegalne, [dostęp: 30.12.2020].

[466] *RODO i kary za wyciek danych – jak uniknąć ryzyka dzięki Microsoft Business 365?*, https://blog.home.pl/2018/11/rodo-i-kary-za-wyciek-danych-jak-uniknac-ryzyka-dzieki-microsoft-business-365/, [dostęp: 30.12.2020].

[467] *50 mln euro kary dla Google za naruszenie RODO*, https://niebezpiecznik.pl/post/50-mln-euro-kary-dla-google-za-naruszenie-rodo/, [dostęp: 30.12.2020].

[468] Zob. *Ogromna kara dla Facebooka. Musi zapłacić 5 mld dolarów. W tle afera z Cambridge Analytica*, https://technologia.dziennik.pl/internet/artykuly/603447,facebook-pieniadze-kara-5-mld-dolarow.html, [dostęp: 30.12.2020]. Por. *Kolejna kara dla Facebooka za naruszenie prywatności*, https://bitdefender.pl/kolejna-kara-dla-facebooka-za-naruszenie-prywatnosci/, [dostęp: 30.12.2020].

16 lipca 2021 roku amerykański koncern Amazon poinformował, że ma zapłacić 887 mln dol. (746 mln euro) za naruszenie unijnych zasad ochrony danych, w spersonalizowanych reklamach. Karę nałożył CNPD (Commission Nationale pour la Protection des Données), właściwy urząd ochrony danych osobowych mający siedzibę w Luksemburgu[469].

W Polsce od wejścia w życie RODO również odnotowano przypadki wydania decyzji przez Prezesa Urzędu Ochrony Danych Osobowych (PUODO) o nałożeniu kary za naruszenie prawa ochrony danych osobowych. Pierwsza kara została nałożona w marcu 2019 roku. PUODO uznał, że spółka z Małopolski naruszyła przepisy RODO poprzez niespełnienie obowiązku informacyjnego względem podmiotów danych. Wysokość kary wyniosła ponad 943 tys. zł. Firma nie kontaktowała się bezpośrednio z osobami, których adresu mailowego nie miała, zamieściła tylko informację na swojej stronie internetowej. Zdaniem Urzędu nie było to wystarczające spełnienie obowiązku informacyjnego[470].

Kolejna kara została nałożona na Dolnośląski Związek Piłki Nożnej, który na swojej stronie internetowej zamieścił dane sędziów z podaniem informacji na temat ich numerów PESEL i miejsca zamieszkania. Mimo prób usunięcia tych informacji przez Związek w trakcie postępowania wyjaśniającego, były one dalej dostępne dla użytkowników Internetu. PUODO uznał to za naruszenie przepisów RODO i wymierzył sankcję wysokości 55.750,50 złotych[471].

Kara nie ominęła również spółkę Morele.net sp. z o.o. prowadzącą sklepy internetowe. Należąca do tego przedsiębiorcy baza danych zawierająca informacje na temat ponad 2 milionów klientów sklepu została wykradziona i opublikowana w Internecie. Ujawnione dane posłużyły do ataków na osoby, których dane dotyczyły (tzw. phishingu). Podstawą prawną nałożenia kary w wysokości 2 830 410 zł. był zarzut naruszenia przez podmiot szeregu norm, w tym poufności danych osobowych (poprzez niezapewnienie bezpieczeństwa przetwarzania danych) oraz legalności, rzetelności i rozliczalności (poprzez niewykazanie, że dane osobowe pochodzące ze zbieranych przez spółkę wniosków ratalnych były przetwarzane na podstawie zgód podmiotów danych)[472].

[469] Zob. *Unia bije w Amazona. Rekordowa kara za naruszenie RODO*, https://cyfrowa.rp.pl/globalne-interesy/art18547121-unia-bije-w-amazona-rekordowa-kara-za-naruszenie-rodo, [dostęp: 30.07.2021]. Por. M. Druś, *Amazon.com ukarany 746 mln EUR za naruszenie RODO*, https://www.pb.pl/amazon-com-ukarany-746-mln-eur-za-naruszenie-rodo-1123493, [dostęp: 30.07.2021].

[470] Zob. *RODO: Pierwsza kara za wyciek danych w następstwie ataku z zewnątrz*, https://www2.deloitte.com/pl/pl/pages/doradztwo-prawne/articles/ochrona-danych-osobowych/newsletter-rodo0/RODO-pierwsza-kara-za-wyciek-danych-w-nastepstwie-ataku-z-zewnatrz.html, [dostęp: 30.12.2020].

[471] Zob. M. Bęza, *Kolejna kara za naruszenie przepisów RODO*, https://home.kpmg/pl/pl/home/insights/2019/10/rodonews-kolejna-kara-za-naruszenie-przepisow-rodo.html, [dostęp: 30.12.2020].

[472] Pierwotną przyczyną wszczęcia postępowania przez Prezesa UODO był wyciek danych klientów, którzy zawiadomili spółkę o otrzymywaniu sms-ów informujących o konieczności dokonania opłaty w wysokości 1 zł, zawierających link do fałszywej bramki płatności. Łącznie wyciek danych dotyczył ponad 2 200 000 użytkowników. W ocenie Prezesa UODO spółka zastosowała niewystarczające środki na poziomie kontroli dostępu i uwierzytelniania do systemów informatycznych i baz danych. W szczególności, zdaniem Prezesa UODO, zastosowany mechanizm uwierzytelniania powinien mieć charakter dwuetapowy (podczas gdy, jak wynika z decyzji Prezesa UODO, Spółka zastosowała mechanizm jednoetapowy). W ocenie organu przedsiębiorcy przetwarzający dane mają obowiązek regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania, tak aby upewnić się, że stosowane przez nich środki odpowiadają rzeczywistemu ryzyku. Zob. J. Greser, *Kary za nieprzestrzeganie przepisów RODO*, https://publicystyka.ngo.pl/kary-za-nieprzestrzeganie-przepisow-rodo, [dostęp: 30.12.2020].

TABELA 14 Administracyjne kary pieniężne nałożone przez PUODO w 2020 r.

L.p.	Data decyzji	Departament prowadzący postępowanie	Sygnatura	Administrator	Wysokość kary w zł
1.	18.02.2020	Departament Skarg	ZSZZS.440.768.2018	Szkoła Podstawowa	20 000,00
2.	20.03.2020	Departament Kontroli i Naruszeń	ZSPR.421.19.2019	Vis Consulting Sp. z o.o.	20 000,00
3.	29.05.2020	Departament Kar i Egzekucji	DKE.561.1.2020	East Power Sp. z o.o.	15 000,00
4.	03.06.2020	Departament Kar i Egzekucji	DKE.561.2.2020	Przedsiębiorca prowadzący przedszkole	5 000,00
5.	02.07.2020	Departament Kar i Egzekucji	DKE.561.3.2020	Główny Geodeta Kraju	100 000,00
6.	21.08.2020	Departament Kontroli i Naruszeń	ZSOŚS.421.25.2019	Szkoła Główna Gospodarstwa Wiejskiego	50 000,00
7.	24.08.2020	Departament Kontroli i Naruszeń	DKN.5112.13.2020	Główny Geodeta Kraju	100 000,00
8.	03.12.2020	Departament Kontroli i Naruszeń	DKN.5112.1.2020	Virgin Mobile Polska Sp. z o.o.	1.968.524,00
9.	09.12.2020	Departament Kar i Egzekucji	DKE.561.13.2020	Smart Cities Sp. z o.o.	12.838,20
10.	09.12.2020	Departament Kontroli i Naruszeń	DKN.5131.5.2020	TUiR Warta S.A.	85.588,00
11.	17.12.2020	Departament Kontroli i Naruszeń	DKN.5130.1354.2020	ID Finance Poland Sp. z o.o. w likwidacji	1.069.850,00

Źródło: *Sprawozdanie z działalności Prezesa Urzędu Ochrony Danych Osobowych w roku 2020*, Prezes Urzędu Ochrony Danych Osobowych

Trafnego podsumowania dotychczasowej linii orzeczniczej organów ochrony danych osobowych w kontekście orzekanych kar dokonał Rafał Malujda. „Analiza przypadków wskazuje na to, że na gruncie przepisów o ochronie danych osobowych negatywnie oceniane są działania o bardzo podstawowym charakterze – niejasna i niepełna treść klauzuli zgody, wykorzystywanie danych zupełnie bez podstawy prawnej czy poza zakresem udzielonej zgody. Można zaryzykować stwierdzenie, iż w takich przypadkach ocena na gruncie RODO

byłaby jednoznaczna. Warto przy tym zauważyć, że skala działania opisanych podmiotów uzasadniała wysokie kary”[473].

Podsumowując należy stwierdzić, że rozporządzenie wprowadziło nieporównywalnie większą siłę „oddziaływania” w zakresie nadzoru sankcyjnego nad prawidłowością przetwarzania danych osobowych. Wcześniejsze kary – wynikające ze starej ustawy o ochronie danych osobowych – były niskie, szczególnie biorąc pod uwagę potencjalną skalę szkód, które można wyrządzić naruszając ochronę danych osobowych w wielkiej skali. Przy tym należy zauważyć, iż po pierwsze nałożenie kary poprzedzała żmudna i długa procedura kontrolna, po drugie karę można było nałożyć jedynie w celu przymuszenia do faktycznego wykonania obowiązków nałożonych na adresata uprzedniej decyzji administracyjnej, po trzecie kary wprowadzono *de facto* dopiero w wyniku nowelizacji z 7 marca 2011 roku. Na mocy art. 12 pkt. 3 starej ustawy Generalny Inspektor Ochrony Danych Osobowych mógł nakładać na podmioty, które nie wykonują jego decyzji administracyjnych grzywny. Zestawienie ówczesnych kar administracyjnych prezentuje graf jak poniżej.

TABELA 15 Kary administracyjne przewidziane ustawą z 1997 roku – porównanie

Źródło: opracowanie własne na podstawie ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz.U. 1997 nr 133 poz. 883 z późn. zm.)

W świetle przepisów ustawy o ochronie danych osobowych z 1997 roku kontrola mogła być przeprowadzona jako: (a) kontrola z urzędu z inicjatywy GIODO, lub (b) kontrola na wniosek – przeprowadzana z inspiracji zewnętrznej (np. Najwyższej Izby Kontroli, Państwowej Inspekcji Pracy, prokuratury, związków zawodowych, pracodawców, czy osoby fizycznej) – co prezentuje graf jak poniżej.

[473] R. Malujda, *Kary za naruszenie przepisów o ochronie danych osobowych*, https://malujda.pl/kary-za-naruszenie-przepisow-o-ochronie-danych-osobowych-ochrona-danych-osobowych/, [dostęp: 30.12.2020].

TABELA 16 Urzędnicy uprawnieni do realizowania kontroli administracyjnej w zakresie ochrony danych osobowych na podstawie porządku prawnego sprzed RODO

Pracownicy Biura GIODO	Pracownicy Państwowej Inspekcji Pracy	Pracownicy Urzędów Marszałkowskich i Wojewódzkich Urzędów Pracy
•na mocy przepisów art. 12-22a ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych •kontrola trwała od kilku do kilkunastu dni i miała charakter kontroli indywidulanej lub sektorowej (kompleksowej lub częściowej)	•na mocy porozumienia zawartego z Generalnym Inspektorem Ochrony Danych Osobowych •kontrola była fragmentaryczna i mogła dotyczyć np.: zakresu upoważnienia do przetwarzania danych osobowych pracownika odpowiadającego za prowadzenie kadr i płac	•na mocy postanowień zawartych w umowach o dofinansowanie realizacji projektów współfinansowanych ze środków UE w ramach EFS zawieranych pomiędzy tymi instytucjami a organizacjami pozarządowymi •kontrola mogła mieć charakter planowy bądź być kontrolą doraźną

Źródło: opracowanie własne na podstawie ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz.U. 1997 nr 133 poz. 883 z późn. zm.) oraz www.giodo.gov.pl [dostęp: 22.12.2020]

Ogląd praktyki kontrolnej z lat 1997–2018 wskazuje, że Generalny Inspektor Ochrony Danych Osobowych ustalał roczne harmonogramy obejmujące kategorie kontrolowanych podmiotów (np. kancelarie prawne, podmioty świadczące usługi medyczne, organy administracji publicznej) lub zagadnień, które były realizowane w danym roku, zarówno w ramach kontroli sektorowej, obejmującej swoim zakresem wszystkie wymogi określone w przepisach, jak i kontroli częściowej, dotyczącej poszczególnych zagadnień w procesie przetwarzania danych (np. będących przedmiotem skargi).

W ramach porządku prawnego, w treści ustawy o ochronie danych osobowych z 1997 roku, momentem wszczęcia postępowania była data podjęcia pierwszej czynności w sprawie wobec podmiotu kontrolowanego[474]. Zakres tematyczny kontroli w pierwszej kolejności sprowadzał się do weryfikacji czy dana instytucja posiadała dokumentację bezpieczeństwa danych osobowych, w tym: (1) Politykę Bezpieczeństwa Danych Osobowych; (2) Instrukcję Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych. Następnie sprawdzana była prawidłowość prowadzenia i aktualizacji ewidencji osób upoważnionych do przetwarzania danych, oraz czy dane osobowe przetwarzały faktycznie osoby posiadające upoważnienie od administratora danych. Podczas kontroli inspektorzy zwracali szczególną uwagę na takie kwestie jak: (a) przesłanki legalności przetwarzania danych osobowych, w tym przesłanki legalności przetwarzania danych wrażliwych, (b) zakres i cel przetwarzania danych (kontrolowany podmiot był obowiązany podać kategorie osób oraz kategorie przetwarzanych danych i ich zakres), (c) merytoryczną poprawność danych i ich adekwatność do celu przetwarzania, (d) dopełnienie obowiązków informacyjnych, (e) zgłoszenie zbioru do rejestracji,

[474] Datą wszczęcia postępowania administracyjnego z urzędu jest data pierwszej czynności organu administracji publicznej dokonanej wobec strony. Czynnością taką będzie zawiadomienie strony (stron) o wszczęciu postępowania na zasadzie art. 61 § 4 K.p.a. Zob. E. Iserzon, J. Starościak, *Kodeks postępowania administracyjnego. Komentarz, teksty, wzory i formularze*, Warszawa 1970, s. 142–143.

(e) udostępnianie, przekazywanie danych, (f) powierzenie przetwarzania danych osobowych, (g) zabezpieczenie danych (inspektorzy oceniali, czy administrator danych zastosował – odpowiednie do zagrożeń oraz kategorii danych – środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych).

Zakres podmiotowy uprawnień kontrolnych w świetle starych przepisów był bardzo szeroki. Kontrola przetwarzania danych osobowych obejmowała zarówno administratorów danych, jak również podmioty, którym na mocy art. 31 ustawy, w drodze umowy zawartej na piśmie powierzono przetwarzanie danych[475]. Kierownik kontrolowanej jednostki organizacyjnej oraz kontrolowana osoba fizyczna będąca administratorem danych byli obowiązani umożliwić inspektorowi przeprowadzenie kontroli, a w szczególności umożliwić przeprowadzenie czynności na miejscu, w tym udostępnić wymagane dokumenty[476]. Z czynności sporządzano protokół, którego jeden egzemplarz doręczany był kontrolowanemu administratorowi danych. Protokół kontroli, podpisywany przez inspektora i kontrolowanego administratora danych, zawierał m.in. zalecenia pokontrolne i czas dany na ich wdrożenie. Administrator mógł wnieść umotywowane zastrzeżenia i uwagi. W razie odmowy podpisania protokołu przez kontrolowanego, inspektor czynił o tym wzmiankę w protokole, a odmawiający mógł, w terminie 7 dni, przedstawić swoje stanowisko na piśmie Generalnemu Inspektorowi.

Na podstawie ustaleń kontroli inspektor mógł po pierwsze żądać wszczęcia postępowania dyscyplinarnego lub innego przewidzianego prawem postępowania przeciwko osobom winnym dopuszczenia do uchybień. Po drugie w przypadku stwierdzenia naruszenia przepisów Generalny Inspektor z urzędu lub na wniosek, w drodze decyzji administracyjnej, nakazywał przywrócenie stanu zgodnego z prawem, a w szczególności: (1) usunięcie uchybień; (2) uzupełnienie, uaktualnienie, sprostowanie, udostępnienie lub nieudostępnienie danych osobowych; (3) zastosowanie dodatkowych środków zabezpieczających zgromadzone dane osobowe; (4) wstrzymanie przekazywania danych osobowych do państwa trzeciego; (5) zabezpieczenie danych lub przekazanie ich innym podmiotom; (6) usunięcie danych osobowych.

W razie stwierdzenia, że działanie lub zaniechanie konkretnej osoby wyczerpywało znamiona przestępstwa określonego w ustawie, Generalny Inspektor kierował do organu wymiaru sprawiedliwości zawiadomienie o możliwości popełnieniu przestępstwa, dołączając dowody dokumentujące podejrzenie.

---

[475] Kontrole przeprowadzane były w zespołach składających się najczęściej z trzech osób – dwóch prawników z Departamentu Inspekcji Biura GIODO oraz jednego informatyka Departamentu Informatyki Biura GIODO. Czynności kontrolne na miejscu były dokonywane w siedzibie kontrolowanego podmiotu oraz w innym miejscu (np. jednostce organizacyjnej) wskazanym jako obszar przetwarzania danych osobowych. Kontroli poddawane były zarówno podmioty sektora publicznego, jak i podmioty prywatne, wskazane jako podmioty zobowiązane do ochrony danych osobowych. Zob. *ABC zasad kontroli przetwarzania danych osobowych, Biuro Generalnego Inspektora Danych Osobowych*, Warszawa 2011, s. 6, file:///C:/Users/adwokat/Downloads/ABC-zasad-kontroli-przetwarzania-danych-osobowych.pdf, [dostęp: 25.11.2020].

[476] Na podstawie ustawy inspektorzy byli wyposażeni m.in. w prawo: (1) wstępu, w godzinach od 6^{00} do 22^{00}, za okazaniem imiennego upoważnienia i legitymacji służbowej, do pomieszczenia, w którym zlokalizowany jest zbiór danych, oraz pomieszczenia, w którym przetwarzane są dane poza zbiorem danych, i przeprowadzenia niezbędnych badań lub innych czynności kontrolnych w celu oceny zgodności przetwarzania danych z ustawą; (2) żądania złożenia pisemnych lub ustnych wyjaśnień oraz wzywać i przesłuchiwać osoby w zakresie niezbędnym do ustalenia stanu faktycznego; (3) wglądu do wszelkich dokumentów i wszelkich danych mających bezpośredni związek z przedmiotem kontroli oraz sporządzania ich kopii; (4) przeprowadzania oględzin urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych; (5) zlecania sporządzanie ekspertyz i opinii. Zob. art. 14 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz.U. 1997 nr 133 poz. 883 z późn. zm.).

Nowa ustawa o ochronie danych osobowych dnia 10 maja 2018 roku wprowadziła rozwiązania prawne dotyczące (1) postępowania w sprawie naruszenia przepisów o ochronie danych osobowych[477], (2) trybu postępowania kontrolnego[478], (3) oraz wysokości i rodzaju administracyjnych kar pieniężnych za naruszenie przepisów o ochronie danych osobowych przez podmioty publiczne. Nowy porządek prawny w zakresie możliwości stosowania sankcji wobec podmiotów publicznych naruszających zasady prawidłowego przetwarzania danych osobowych przewiduje nieporównywalnie niższe kary, niż wobec podmiotów komercyjnych (regulowanych przez RODO). I tak Prezes Urzędu Ochrony Danych Osobowych, zgodnie z art. 101 ustawy, może nałożyć na podmiot obowiązany do przestrzegania przepisów rozporządzenia 2016/679, inny niż: 1) jednostka sektora finansów publicznych, 2) instytut badawczy, 3) Narodowy Bank Polski – w drodze decyzji, administracyjną karę pieniężną na podstawie i na warunkach określonych w art. 83 rozporządzenia 2016/679[479]

Prezes Urzędu może nałożyć, w drodze decyzji, administracyjne kary pieniężne w wysokości do 100 000 złotych, na: (1) jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 1–12 i 14 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych; (2) instytut badawczy; (3) Narodowy Bank Polski. Prezes Urzędu może nałożyć, w drodze decyzji, administracyjne kary pieniężne w wysokości do 10 000 złotych na jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 13 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (tj. do 10 000 złotych na państwowe i samorządowe instytucje kultury)[480].

Równowartość wyrażonych w euro kwot, o których mowa w art. 83 rozporządzenia 2016/679, oblicza się w złotych według średniego kursu euro ogłoszonego przez Narodowy Bank Polski w tabeli kursów na dzień 28 stycznia każdego roku, a w przypadku gdy w danym roku Narodowy Bank Polski nie ogłasza średniego kursu euro w dniu 28 stycznia – według średniego kursu euro ogłoszonego w najbliższej po tej dacie tabeli kursów Narodowego Banku Polskiego. Karę pieniężną uiszcza się w terminie 14 dni od dnia upływu terminu na wniesienie skargi, albo od dnia uprawomocnienia się orzeczenia sądu administracyjnego. W razie upływu terminu tego terminu kara pieniężna podlega ściągnięciu w trybie przepisów o postępowaniu egzekucyjnym w administracji[481].

[477] Szerzej zob. P. Litwiński, *Ochrona danych osobowych w ogólnym postępowaniu administracyjnym*, wyd. I, Wolters Kluwer, Warszawa 2009.

[478] Por. A. Mednis, K. Rudzińska, *Przetwarzanie danych osobowych podczas postępowania kontrolnego prowadzonego przez Najwyższą Izbę Kontroli*, Przegląd Metodyczny 2012, nr 3.

[479] W wersji projektu ustawy z dn. 10 maja 2018 r. jak następuje. na podmioty niebędące organami publicznymi w rozumieniu w art. 5 § 2 pkt 3 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego albo podmiotami publicznymi w rozumieniu w art. 9 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych, w drodze decyzji, administracyjne kary pieniężne na podstawie i na warunkach określonych w art. 83 rozporządzenia. Zob. Opracowanie własne na podstawie projektu ustawy o ochronie danych osobowych skierowany na Komitet do Spraw Europejskich Rady Ministrów, https://www.gov.pl/web/cyfryzacja/projekt-ustawy-o-ochronie-danych-osobowych-skierowany-na-komitet-do-spraw-europejskich-rady-ministrow, [dostęp: 02.12.2021].

[480] Równowartość wyrażonych w euro kwot administracyjnych kar pieniężnych oblicza się według średniego kursu euro ogłaszanego przez Narodowy Bank Polski w tabeli kursów na dzień 28 stycznia każdego roku, kiedy obchodzony jest Dzień Ochrony Danych Osobowych. Środki nie zasilają samego Urzędu. Administracyjną karę pieniężną uiszcza się w terminie 14 dni od dnia upływu terminu na wniesienie skargi do Wojewódzkiego Sądu Administracyjnego w Warszawie albo od dnia uprawomocnienia się orzeczenia sądu administracyjnego. Na wniosek podmiotu ukaranego Prezes UODO może odroczyć termin uiszczenia administracyjnej kary pieniężnej albo rozłożyć ją na raty jeżeli przemawia za tym ważny interes wnioskodawcy. Zob. G. Rychły, *Administracyjne kary pieniężne nakładane przez PUODO*, https://mojafirma.infor.pl/biznes/prawo/rodo-w-firmie/3101901,Administracyjne-kary-pieniezne-nakladane-przez-PUODO.html, [dostęp: 15.12.2020].

[481] Prezes Urzędu może na wniosek podmiotu ukaranego odroczyć uiszczenie kary pieniężnej albo rozłożyć ją na raty ze względu na ważny interes wnioskodawcy. Do wniosku dołącza się uzasadnienie. W przypadku odroczenia terminu uiszczenia administracyjnej kary pieniężnej albo rozłożenia jej na raty, Prezes Urzędu nalicza od nieuiszczonej kwoty odsetki w stosunku rocznym, przy zastosowaniu obniżonej stawki odsetek za zwłokę, ogłaszanej na podstawie art. 56d ustawy z dnia 29 sierpnia 1997 r. – Ordynacja podatkowa (Dz. U. z 2018 r. poz. 800, 650, 723, 771 i 1000), od dnia następującego po dniu złożenia wniosku. W przypadku rozłożenia na raty kary pieniężnej, odsetki, o których mowa w ust. 3, są naliczane odrębnie dla każdej raty. Odsetki są naliczane

Projektodawca w pierwotnym brzmieniu ustawy powoływał do życia Fundusz Ochrony Danych Osobowych, którego dysponentem miał być Prezes Urzędu. Fundusz miał być państwowym funduszem celowym, a przychodami Funduszu miały być środki finansowe pochodzące z 1% kar pieniężnych nakładanych przez Prezesa Urzędu[482]. Ostatecznie przepis art. 104 ustawy stanowi wprost, że środki z administracyjnej kary pieniężnej stanowią dochód budżetu państwa *ergo* pomysł na powołanie Funduszu nie wytrzymał próby czasu.

Sankcje są nakładane w toku postępowania w sprawie naruszenia przepisów o ochronie danych osobowych. Jednoinstancyjne postępowanie wszczynane – tak jak wcześniej – jest z urzędu, lub na wniosek[483]. Postępowanie jest prowadzone przez Prezesa Urzędu ds. Ochrony Danych Osobowych. Prezes Urzędu dysponuje przywilejem dostępu do wszelkich informacji, w tym danych osobowych, niezbędnych do prowadzenia postępowania, w tym może żądać od strony przedstawienia tłumaczenia na język polski sporządzonej w języku obcym dokumentacji przedłożonej przez stronę[484]. Jeżeli w toku postępowania zostanie uprawdopodobnione, że przetwarzanie danych osobowych narusza przepisy o ochronie danych osobowych, a dalsze ich przetwarzanie może spowodować poważne i trudne do usunięcia skutki, Prezes Urzędu w celu zapobieżenia tym skutkom może, w drodze postanowienia, zobowiązać podmiot (któremu jest zarzucane naruszenie przepisów o ochronie danych osobowych) do ograniczenia przetwarzania danych osobowych wskazując dopuszczalny zakres tego przetwarzania[485]. Postanowienie to obowiązuje nie dłużej niż do czasu wydania decyzji kończącej postępowanie w sprawie. W toku postępowania Prezes Urzędu ma prawo nałożenia kary grzywny do 500 zł. w sytuacji gdy mimo prawidłowego wezwania bez uzasadnionej przyczyny świadek lub biegły nie stawił się albo bezzasadnie odmówił złożenia zeznania, przedstawienia tłumaczenia na język polski sporządzonej w języku obcym dokumentacji

za okres od dnia upływu odroczonego terminu płatności kary pieniężnej albo terminu zapłaty poszczególnych rat. Prezes Urzędu może uchylić odroczenie uiszczenia kary pieniężnej albo rozłożenie jej na raty, jeżeli ujawniły się nowe lub uprzednio nieznane okoliczności istotne dla rozstrzygnięcia lub jeżeli rata nie została uiszczona w terminie. Rozstrzygnięcie Prezesa Urzędu w przedmiocie odroczenia uiszczenia kary pieniężnej albo rozłożenia jej na raty następuje w drodze postanowienia, na które nie przysługuje skarga do sądu administracyjnego. Zob. art. 105 ustawy z 10 maja 2018 o ochronie danych osobowych (t.j. Dz.U. 2019 r., poz. 1781).

[482] Wydatki Funduszu miały być przeznaczone na: (1) inicjowanie i podejmowanie przez Prezesa Urzędu przedsięwzięć w zakresie upowszechniania w społeczeństwie wiedzy o potrzebie ochrony danych osobowych oraz ryzyku, przepisach, zabezpieczeniach i prawach związanych z ich przetwarzaniem. Szczególną uwagę poświęca się działaniom skierowanym do dzieci, (2) inicjowanie i podejmowanie przez Prezesa Urzędu przedsięwzięć w zakresie upowszechniania wśród administratorów i podmiotów przetwarzających wiedzy o obowiązkach spoczywających na nich na mocy przepisów o ochronie danych osobowych. Zob. Projekt ustawy o ochronie danych osobowych z dnia 28 marca 2017 roku, https://www.gov.pl/web/cyfryzacja/projekt-ustawy-o-ochronie-danych-osobowych, [dostęp: 05.12.2021].

[483] Gdy prawa osoby przysługujące na mocy przepisów o ochronie danych osobowych zostały naruszone, organizacja społeczna może występować z żądaniem: 1) wszczęcia postępowania, 2) dopuszczenia jej do udziału w postępowaniu, jeżeli jest to uzasadnione celami statutowymi tej organizacji i gdy przemawia za tym interes osoby, której prawa zostały naruszone. Zob. art. 31 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (t.j. Dz.U. z 2021 r., poz. 735).

[484] Prawo to podlega ograniczeniu ze względu na tajemnice ustawowo chronione. Strona może zastrzec informacje, dokumenty lub ich części zawierające tajemnicę przedsiębiorstwa. Prezes Urzędu może uchylić zastrzeżenie w drodze decyzji, jeżeli uzna, że informacje, dokumenty lub ich części nie spełniają przesłanek do objęcia ich tajemnicą przedsiębiorstwa. W przypadku ustawowego obowiązku przekazania informacji lub dokumentów otrzymanych od przedsiębiorców innym krajowym lub zagranicznym organom lub instytucjom, informacje i dokumenty przekazuje się wraz z zastrzeżeniem i pod warunkiem jego przestrzegania. Prezes Urzędu na wniosek lub z urzędu może, w drodze postanowienia, w niezbędnym zakresie ograniczyć prawo wglądu do materiału dowodowego, jeżeli udostępnienie tego materiału groziłoby ujawnieniem tajemnicy przedsiębiorstwa, lub innych tajemnic podlegających ochronie na podstawie odrębnych przepisów. Zob. art. 65 ustawy z 10 maja 2018 o ochronie danych osobowych (t.j. Dz.U. z 2019 r., poz. 1781). Szerzej por. A. Krasuski, D. Skolimowska, *Dane osobowe w przedsiębiorstwie*, Warszawa 2007.

[485] Zob. art 16–19 ustawy z 10 maja 2018 o ochronie danych osobowych (t.j. Dz.U. z 2019 r., poz. 1781). Należy zauważyć, że art. 24 ust. 1 projektu ustawy ochronie danych osobowych z dnia 28 marca 2017 roku wskazywał, że nowy organ nadzorczy będzie dysponował możliwością wydania postanowienia, zobowiązującego podmiot, któremu jest zarzucane naruszenie przepisów o ochronie danych osobowych, do ograniczenia przetwarzania danych osobowych – jeszcze przed wydaniem decyzji kończącej postępowanie. W ostatecznym kształcie prawnym PUODO może wydać decyzję np. nakazującą usunięcie danych osobowych dopiero po zakończeniu postępowania, przy czym podmiot, wobec którego taką decyzję wydano jest zobowiązany do jej realizacji dopiero po jej uprawomocnieniu. Zob. Projekt ustawy o ochronie danych osobowych z dnia 28 marca 2017 roku, https://www.gov.pl/web/cyfryzacja/projekt-ustawy-o-ochronie-danych-osobowych, [dostęp: 05.12.2021].

przedłożonej przez stronę, wydania opinii, okazania przedmiotu oględzin albo udziału w innej czynności urzędowej.

W toku wyżej opisanego postępowania lub niezależnie od niego może być prowadzone przez Prezesa Urzędu postępowanie kontrolne, które jest postępowaniem odrębnym od postępowania prowadzonego w związku z naruszeniem przepisów o ochronie danych osobowych[486]. Podobnie jak wcześniej postępowanie kontrolne może być prowadzone zgodnie z zatwierdzonym przez Prezesa Urzędu planem kontroli bądź poza planem na podstawie uzyskanych przez Prezesa Urzędu informacji albo przeprowadzonych analiz. Kontrola jest przeprowadzona przez upoważnionego pracownika Urzędu, przy czym do przeprowadzania kontroli Prezes Urzędu może upoważnić członka lub pracownika organu nadzorczego państwa członkowskiego UE w przypadku, o którym mowa w art. 62 rozporządzenia[487].

Upoważnienie do przeprowadzenia kontroli zawiera: (1) wskazanie podstawy prawnej przeprowadzenia kontroli, (2) oznaczenie organu kontroli, (3) imię i nazwisko, stanowisko służbowe osoby upoważnionej do przeprowadzenia kontroli oraz numer jej legitymacji służbowej, (4) określenie zakresu przedmiotowego kontroli, w tym okresu objętego kontrolą, (5) oznaczenie podmiotu objętego kontrolą, (6) wskazanie daty rozpoczęcia i przewidywanego terminu zakończenia czynności kontrolnych, (7) podpis Prezesa Urzędu, (8) pouczenie podmiotu objętego kontrolą o jego prawach i obowiązkach, (9) datę i miejsce wystawienia imiennego upoważnienia[488].

Podstawowe kompetencje kontrolerów w związku z podejmowanymi czynnościami są niemal identyczne jak w przypadku wcześniejszego systemu. I tak w celu uzyskania niezbędnych informacji mogących stanowić dowód w sprawie kontrolujący ma prawo:

1) wstępu w godzinach od 6^{00} do 22^{00} na grunt oraz do budynków, lokali, pomieszczeń,
2) wglądu do dokumentów i informacji mających bezpośredni związek z kontrolś,
3) przeprowadzania oględzin miejsc, przedmiotów, urządzeń, nośników oraz systemów informatycznych lub teleinformatycznych służących do przetwarzania danych,
4) żądać złożenia pisemnych lub ustnych wyjaśnień oraz przesłuchiwać w charakterze świadka osoby w zakresie niezbędnym do ustalenia stanu faktycznego,
5) zlecać sporządzanie ekspertyz i opinii.

Kontrolowany zapewnia kontrolującemu oraz osobom upoważnionym do udziału w kontroli warunki i środki niezbędne do sprawnego przeprowadzenia kontroli, a w szczególności sporządza we własnym zakresie kopie lub wydruki dokumentów oraz informacji

[486] Do kontroli działalności gospodarczej przedsiębiorcy, stosuje się przepisy rozdziału 5 ustawy z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej, z wyłączeniem przepisów art. 79, art. 82 i art. 83. Zob. *Prawo gospodarcze. Zagadnienia administracyjnoprawne*, red. H. Gronkiewicz-Waltz, M. Wierzbowski Warszawa 2015.

[487] Kontrolujący podlega wyłączeniu z udziału w kontroli, na wniosek lub z urzędu, jeżeli: wyniki kontroli mogłyby oddziaływać na prawa lub obowiązki jego, jego małżonka, osoby pozostającej z nim faktycznie we wspólnym pożyciu, krewnego i powinowatego do drugiego stopnia albo na osoby związanej z nim z tytułu przysposobienia, opieki albo kurateli, lub zachodzą uzasadnione wątpliwości co do jego bezstronności. Powody wyłączenia trwają także po ustaniu małżeństwa, przysposobienia, opieki lub kurateli. O wyłączeniu kontrolującego rozstrzyga Prezes Urzędu. Do czasu wydania postanowienia kontrolujący podejmuje czynności niecierpiące zwłoki. Zob. art. 80 ustawy z 10 maja 2018 o ochronie danych osobowych (t.j. Dz.U. 2019 r., poz. 1781). Por. K. Rokita, *Niezależność organów ochrony danych osobowych w ogólnym rozporządzeniu o ochronie danych*, Europejski Przegląd Sądowy 2016, nr 7, s. 4–12.

[488] Art. 81 ustawy z 10 maja 2018 o ochronie danych osobowych (t.j. Dz.U. z 2019 r., poz. 1781).

zgromadzonych na nośnikach, w urządzeniach lub systemach. Kontrolowany dokonuje potwierdzenia za zgodność z oryginałem sporządzonych kopii lub wydruków. W przypadku odmowy potwierdzenia za zgodność z oryginałem kontrolujący czyni o tym wzmiankę w protokole kontroli. W uzasadnionych przypadkach przebieg kontroli lub poszczególne czynności w jej toku, po uprzednim poinformowaniu kontrolowanego, mogą być utrwalane przy pomocy urządzeń rejestrujących obraz lub dźwięk. Informatyczne nośniki danych w rozumieniu ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[489].

Zmiana w stosunku do starej ustawy obejmuje uprawnienia kontrolującego do dokonania czynności przesłuchania pracownika kontrolowanego w charakterze świadka[490]. Do przesłuchania pracownika kontrolowanego stosuje się przepis art. 83 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego[491].

Prezes Urzędu lub kontrolujący może zwrócić się do właściwego miejscowo komendanta Policji o pomoc, jeżeli jest to niezbędne do wykonywania czynności kontrolnych. Policja udziela pomocy przy wykonywaniu czynności kontrolnych, po otrzymaniu pisemnego wezwania na co najmniej 7 dni przed terminem tych czynności. W pilnych przypadkach, w szczególności gdy kontrolujący trafi na opór uniemożliwiający lub utrudniający wykonywanie czynności kontrolnych, udzielenie pomocy następuje również na ustne wezwanie Prezesa Urzędu lub kontrolującego, po okazaniu imiennego upoważnienia do przeprowadzenia kontroli oraz legitymacji służbowej kontrolującego. W pilnych przypadkach, Prezes Urzędu przekazuje potwierdzenie wezwania na piśmie, nie później niż w terminie 3 dni po zakończeniu czynności kontrolnych. Udzielenie pomocy Policji przy wykonywaniu czynności kontrolnych polega na zapewnieniu kontrolującemu bezpieczeństwa osobistego oraz dostępu do miejsca wykonywania kontroli i porządku w tym miejscu. Policja, udzielając pomocy kontrolującemu przy wykonywaniu czynności kontrolnych, zapewnia bezpieczeństwo również innym osobom uczestniczącym przy wykonywaniu czynności kontrolnych, mając w szczególności na względzie poszanowanie godności osób biorących udział w kontroli. Koszty poniesione przez Policję z tytułu udzielonej pomocy przy wykonywaniu czynności kontrolnych rozlicza się według stawki zryczałtowanej w wysokości 1,5% przeciętnego miesięcznego wynagrodzenia w sektorze przedsiębiorstw bez wypłat nagród z zysku za ubiegły rok, ogłaszanego

[489] Do nowelizacji z 2019 roku przepis wprowadzał następujące uprawnienia: (1) wstępu na grunt oraz do budynków, lokali lub innych pomieszczeń, (2) wglądu do wszelkich dokumentów i wszelkich informacji mających bezpośredni związek z przedmiotem kontroli, (3) przeprowadzania oględzin urządzeń, nośników oraz systemów informatycznych lub teleinformatycznych służących do przetwarzania danych, (4) żądać złożenia pisemnych lub ustnych wyjaśnień oraz wzywać i przesłuchiwać w charakterze świadka osoby w zakresie niezbędnym do ustalenia stanu faktycznego. Zob. art. 84 ustawy z 10 maja 2018 o ochronie danych osobowych (t.j. Dz.U. 2018 poz. 1000).

[490] Utrwalony pogląd dot. czynności kontrolnych (np. prawo ochrony konkurencji i konsumentów – art. 105b) wskazuje, że przed rozpoczęciem przesłuchania kontrolujący obowiązany jest uprzedzić świadka o odpowiedzialności karnej za zeznanie nieprawdy lub zatajenie prawdy. Osoba ta może jednak odmówić udzielenia informacji lub współdziałania w toku kontroli tylko wtedy, gdy naraziłoby to ją lub jej małżonka, wstępnych, zstępnych, rodzeństwo oraz powinowatych w tej samej linii lub stopniu, jak również osoby pozostające w stosunku przysposobienia, opieki lub kurateli, a także osobę pozostającą we wspólnym pożyciu, na odpowiedzialność karną. Prawo odmowy udzielenia informacji lub współdziałania w toku kontroli trwa po ustaniu małżeństwa lub rozwiązaniu stosunku przysposobienia, opieki lub kurateli. Zob. art. 105d ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (t.j. Dz.U. z 2021r., poz. 275). Tak też w projekcie ustawy o ochronie danych osobowych z dnia 28 marca 2017 roku, https://www.gov.pl/web/cyfryzacja/projekt-ustawy-o-ochronie-danych-osobowych, [dostęp: 05.12.2021].

[491] Art. 86 ustawy z 10 maja 2018 o ochronie danych osobowych (t.j. Dz.U. z 2019 r., poz. 1781).

przez Prezesa Głównego Urzędu Statystycznego na podstawie art. 60 pkt 5 ustawy z dnia 15 lipca 2011 r. o zawodach pielęgniarki i położnej[492].

Stan faktyczny będący podstawą do przedstawienia wyników z kontroli może być ustalony wyłącznie na podstawie dowodów zebranych w toku kontroli, a w szczególności dokumentów, przedmiotów, oględzin oraz ustnych lub pisemnych wyjaśnień i oświadczeń[493]. Przebieg przeprowadzonej kontroli kontrolujący przedstawia w protokole kontroli. Protokół kontroli powinien zawierać: (1) wskazanie nazwy albo imienia i nazwiska oraz adresu kontrolowanego, (2) imię i nazwisko osoby reprezentującej podmiot kontrolowany oraz nazwę organu reprezentującego ten podmiot, (3) imię i nazwisko, stanowisko służbowe, numer legitymacji służbowej oraz numer upoważnienia kontrolującego, (4) datę rozpoczęcia i zakończenia czynności kontrolnych, (5) określenie przedmiotu i zakresu kontroli, (6) opis stanu faktycznego ustalonego w toku kontroli oraz inne informacje mające istotne znaczenie dla oceny zgodności przetwarzania danych z przepisami o ochronie danych osobowych, (7) wyszczególnienie załączników, (8) omówienie dokonanych w protokole poprawek, skreśleń i uzupełnień, (9) informację o pouczeniu kontrolowanego o prawie zgłaszania zastrzeżeń do protokołu oraz o prawie odmowy podpisania protokołu, (10) datę i miejsce podpisania protokołu przez kontrolującego i kontrolowanego[494].

Protokół kontroli podpisują kontrolujący i kontrolowany. Kontrolowany w terminie 7 dni od dnia przedstawienia protokołu kontroli do podpisu podpisuje go albo składa pisemne zastrzeżenia do jego treści. W przypadku złożenia zastrzeżeń, kontrolujący dokonuje ich analizy i, w razie potrzeby, podejmuje dodatkowe czynności kontrolne, a w przypadku stwierdzenia zasadności zastrzeżeń zmienia lub uzupełnia odpowiednią część protokołu kontroli w formie aneksu do protokołu kontroli. W razie nieuwzględnienia zastrzeżeń w całości albo części, kontrolujący przekazuje kontrolowanemu informacje o tym wraz z uzasadnieniem. Brak doręczenia kontrolującemu podpisanego protokołu kontroli i niezgłoszenie zastrzeżeń do jego treści w terminie 7 dni, uznaje się za odmowę podpisania protokołu kontroli. O odmowie podpisania protokołu kontroli kontrolujący czyni wzmiankę w tym protokole, zawierającą datę jej dokonania. W przypadku, o którym mowa w ust. 7, wzmianki dokonuje się po upływie terminu 7 dni. Protokół kontroli sporządza się w postaci elektronicznej albo w postaci papierowej w dwóch egzemplarzach. Protokół kontroli kontrolujący doręcza kontrolowanemu[495].

Przed podpisaniem protokołu kontrolowany może, w terminie 7 dni od przedstawienia mu go do podpisu, złożyć pisemne zastrzeżenia do tego protokołu. W razie zgłoszenia zastrzeżeń kontrolujący dokonuje ich analizy i, w razie potrzeby, podejmuje dodatkowe czynności kontrolne, a w przypadku stwierdzenia zasadności zastrzeżeń zmienia lub uzupełnia odpowiednią część protokołu w formie aneksu do protokołu. W razie nieuwzględnienia zastrzeżeń w całości

[492] Art. 85 ustawy z 10 maja 2018 o ochronie danych osobowych (t.j. Dz.U. 2019 r., poz. 1781).
[493] Art.. 87 ustawy z 10 maja 2018 o ochronie danych osobowych (t.j. Dz.U. 2019 r., poz. 1781).
[494] Art. 88 ust. 2 ustawy z 10 maja 2018 o ochronie danych osobowych (t.j. Dz.U. 2019 r., poz. 1781).
[495] Art. 88 ust. 3–9 ustawy z 10 maja 2018 o ochronie danych osobowych (t.j. Dz.U. 2019 r., poz. 1781).

lub w części kontrolujący informuje o tym kontrolowanego na piśmie. O odmowie podpisania protokołu kontrolujący czyni wzmiankę w protokole, zawierającą datę jej dokonania. Protokół w postaci papierowej sporządza się w dwóch egzemplarzach, z których jeden pozostawia się kontrolowanemu, a w przypadku protokołu sporządzonego w postaci elektronicznej doręcza się go kontrolowanemu.

Kontrolę prowadzi się nie dłużej niż 30 dni od dnia okazania kontrolowanemu lub innej osobie wskazanej w przepisach imiennego upoważnienia do przeprowadzenia kontroli oraz legitymacji służbowej lub innego dokumentu potwierdzającego tożsamość. Do terminu nie wlicza się terminów przewidzianych na zgłoszenie zastrzeżeń do protokołu lub podpisanie i doręczenie protokołu kontroli przez kontrolowanego. Terminem zakończenia kontroli jest dzień podpisania protokołu przez kontrolowanego albo dzień dokonania wzmianki[496].

Na podstawie ustaleń kontroli Prezes Urzędu może żądać wszczęcia postępowania dyscyplinarnego lub innego przewidzianego prawem postępowania przeciwko osobom winnym uchybień i poinformowania go, w określonym terminie, o wynikach tego postępowania i podjętych działaniach. W razie stwierdzenia, że działanie lub zaniechanie wyczerpuje znamiona przestępstwa określonego w ustawie, Prezes Urzędu kieruje do organu powołanego do ścigania przestępstw zawiadomienie o popełnieniu przestępstwa, dołączając dowody dokumentujące podejrzenie. Jeżeli na podstawie informacji zgromadzonych w protokole kontroli, Prezes Urzędu uzna, że mogło dojść do naruszenia przepisów o ochronie danych osobowych, obowiązany jest do niezwłocznego wszczęcia postępowania w sprawie naruszenia przepisów.

W przypadku naruszenia przepisów o ochronie danych osobowych Prezes Urzędu, w drodze decyzji podejmuje rozstrzygnięcia, których katalog przewiduje rozporządzenie, w tym może administratorowi lub podmiotowi przetwarzającemu dane:

1) wydać ostrzeżenie dotyczące możliwości naruszenia przepisów;
2) udzielić upomnienia;
3) nakazać spełnienie żądania osoby, której dane dotyczą, wynikającego z praw przysługujących jej na mocy rozporządzenia;
4) nakazać dostosowanie operacji przetwarzania do przepisów rozporządzenia;
5) nakazać zawiadomienie osoby, której dane dotyczą, o naruszeniu ochrony danych;
6) wprowadzić czasowe lub całkowite ograniczenie przetwarzania (zakaz przetwarzania);
7) nakazać sprostowanie lub usunięcie danych osobowych lub ograniczenie ich przetwarzania oraz nakazać powiadomienie o tych czynnościach odbiorców, którym dane osobowe ujawniono;
8) cofnąć certyfikację lub nakazać podmiotowi certyfikującemu cofnięcie udzielonej certyfikacji, lub nakazać podmiotowi certyfikującemu nieudzielania certyfikacji, jeżeli jej wymogi nie są spełnione lub przestały być spełniane;
9) zastosować, oprócz lub zamiast ww. środków, administracyjną karę pieniężną;

[496] Art. 89 ustawy z 10 maja 2018 o ochronie danych osobowych (t.j. Dz.U. 2019 r., poz. 1781).

10) nakazać zawieszenia przepływu danych do odbiorcy w państwie trzecim lub do organizacji międzynarodowej[497].

W przypadku gdy waga naruszenia przepisów jest znikoma, a strona zaprzestała dokonywania naruszeń Prezes Urzędu może, w drodze decyzji udzielić upomnienia. W przypadku gdy podmiot, do którego skierowany jest nakaz zawarty w decyzji organu, nie wykona obowiązku wynikającego z tej decyzji, Prezes Urzędu może zastosować środki egzekucyjne w celu przymuszenia do wykonania obowiązku, zgodnie z przepisami ustawy o postępowaniu egzekucyjnym w administracji. Jednocześnie Prezes Urzędu jest kompetentny do wydania decyzji administracyjnej zawierającej nakaz przywrócenia stanu zgodnego z prawem. Aby wydanie decyzji kończącej postępowanie, nakazującej przywrócenie stanu zgodnego z prawem było dopuszczalne, naruszenie powinno istnieć w dniu wydawania decyzji. Jednakże, nawet w przypadku usunięcia nieprawidłowości, organ nadzorczy może nałożyć karę pieniężną za zaistniałe naruszenie ochrony danych[498].

Zgodnie z art. 73 ustawy Prezes Urzędu, jeżeli uzna, że przemawia za tym interes publiczny, po zakończeniu postępowania informuje o wydaniu decyzji na swojej stronie podmiotowej w Biuletynie Informacji Publicznej. Jednostki sektora finansów publicznych, instytuty badawcze oraz Narodowy Bank Polski, w stosunku do których Prezes Urzędu wydał prawomocną decyzję stwierdzającą naruszenie, niezwłocznie podają do publicznej wiadomości na swojej stronie internetowej lub stronie podmiotowej w Biuletynie Informacji Publicznej, informację o działaniach podjętych w celu wykonania decyzji[499].

Na podstawie art. 127 § 3 Kodeksu postępowania administracyjnego od decyzji przysługuje stronie prawo do wniesienia wniosku o ponowne rozpatrzenie sprawy w terminie 14 dni od dnia jej doręczenia stronie. Decyzje ostateczne wydane przez Prezesa Urzędu podlegają natychmiastowemu wykonaniu[500].

---

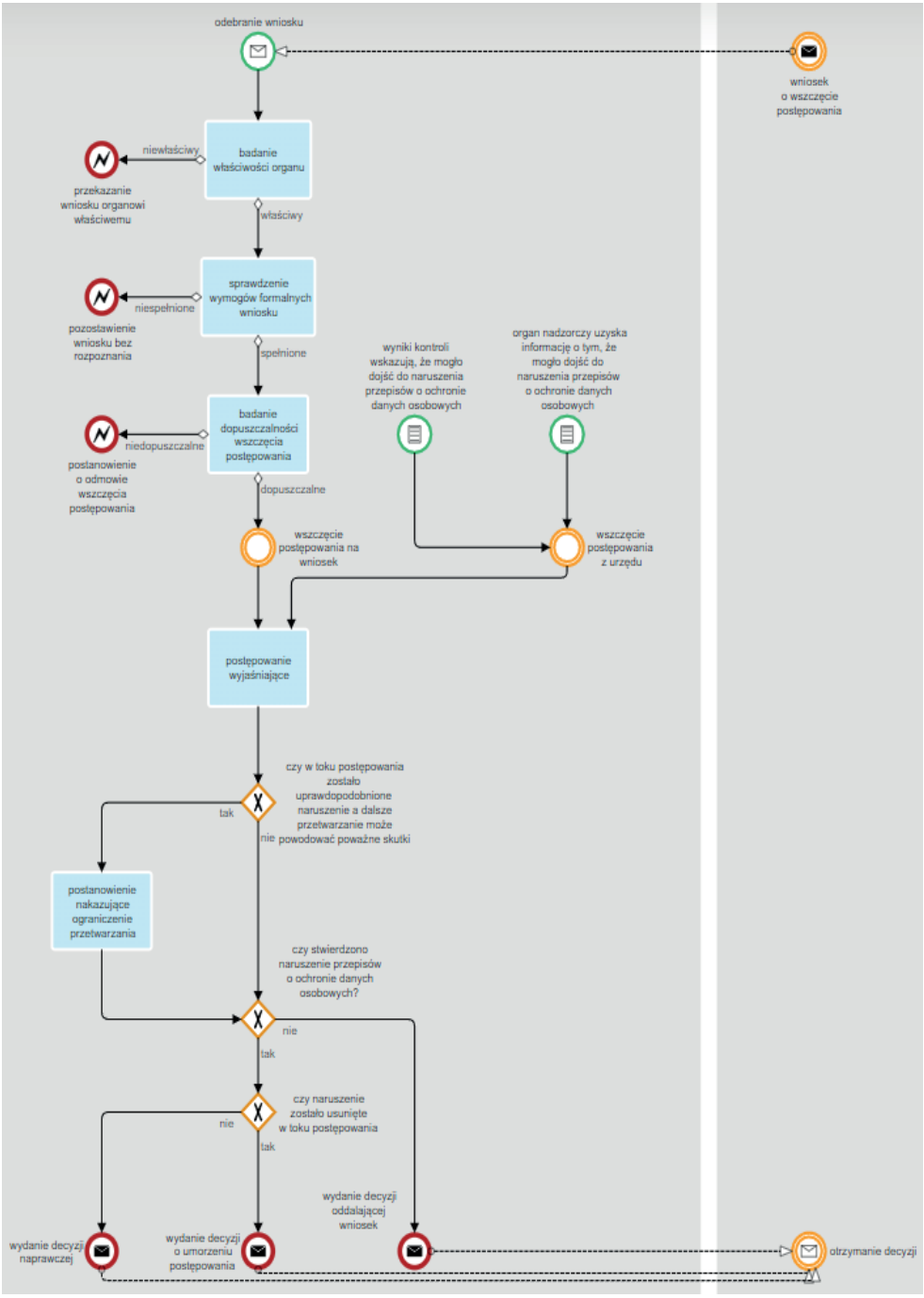
[497] Zob. art. 58 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. UE L 119 z dn. 4.05.2016, s. 1–88).

[498] Zob. postępowanie w sprawie naruszenia przepisów o ochronie danych osobowych prowadzone przez Prezesa Urzędu Ochrony Danych Osobowych. P. Fajgielski, *Prawo ochrony danych osobowych Zarys wykładu*, Wolters Kluwer, Warszawa 2019, s. 189–192.

[499] W projekcie ustawy z 2017 roku przepis brzmiał następująco. W przypadku podjęcia przez Prezesa Urzędu w drodze decyzji rozstrzygnięć, o których mowa w art. 58 ust. 2 lit. b-g i lit. j rozporządzenia 2016/679, wobec organów, o których mowa w art. 5 § 2 pkt 3 Kodeksu postępowania administracyjnego albo podmiotów publicznych, o których mowa w art. 9 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych. Prezes Urzędu udostępnia prawomocne decyzje w Biuletynie Informacji Publicznej na swojej stronie podmiotowej. Do udostępniania decyzji, o których mowa w ust. 1, stosuje się przepisy art. 5 ust. 1 i 2 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej. Organy, o których mowa w art. 5 § 2 pkt 3 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego a także podmioty publiczne, o których mowa w art. 9 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych, niezwłocznie udostępniają na swoich stronach internetowych informacje o działaniach podjętych w celu wykonania decyzji, o których mowa w ust. 1. Zob. art. 57 projektu ustawy o ochronie danych osobowych z dnia 28 marca 2017 roku, https://www.gov.pl/web/cyfryzacja/projekt-ustawy-o-ochronie-danych-osobowych, [dostęp: 05.12.2021]. Szerzej na temat udostępniania informacji publicznej zob. M. Sakowska-Baryła, *Orzecznictwo w sprawie udostępniania i odmowy udostępnienia informacji publicznej*, wyd. I, Municipium S.A, Warszawa 2010.

[500] RODO zawiera wskazówki co do karania osób fizycznych: Aby egzekwowanie przepisów rozporządzenia było skuteczniejsze, należy za jego naruszenie nakładać sankcje, w tym administracyjne kary pieniężne – oprócz lub zamiast odpowiednich środków nakładanych na mocy 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. Zob. Motyw 148 preambuły 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 (Dz. Urz. UE L 119 z dn. 4.05.2016, s. 1–88).

RYSUNEK 20 Drzewo postępowania w sprawie naruszenia przepisów o ochronie danych osobowych przed PUODO



Źródło: P. Fajgielski, *Prawo ochrony danych osobowych Zarys wykładu*, Wolters Kluwer, Warszawa 2019, s. 191

Postanowienia strona może zaskarżyć w skardze na decyzję Prezesa Urzędu. Rozporządzenie zobowiązuje państwa członkowskie do zabezpieczenia proceduralnych środków kontroli nad działalnością organu nadzorczego w zakresie nakładania kar, obejmujących prawo do skutecznego sądowego środka ochrony prawnej i rzetelnego procesu. W Polsce kontrolę sądową w zakresie kar sprawują sądy administracyjne. Należy zauważyć, że była także rozważana inna koncepcja kontroli nad działalnością organu nadzorczego. Przykładem mogą tu być sektory regulowane odrębnymi ustawami, takie jak sektor telekomunikacyjny. Charakteryzuje się on dwoistym trybem kontroli: sprawują ją co do zasady sądy administracyjne, z wyjątkiem spraw dotyczących kontroli konkurencji i nakładanych przez organ regulacyjny kar. Ten drugi aspekt podlega kontroli Sądu Ochrony Konkurencji i Konsumentów[501]. Jeżeli strona nie chce skorzystać z prawa do złożenia wniosku o ponowne rozpatrzenie sprawy, ma prawo do wniesienia skargi na decyzję do Wojewódzkiego Sądu Administracyjnego w Warszawie w terminie 30 dni od dnia doręczenia jej stronie. Skargę wnosi się za pośrednictwem Prezesa Urzędu Ochrony Danych Osobowych. Wpis od skargi wynosi 200 złotych. Wniesienie przez stronę skargi do sądu administracyjnego powoduje wstrzymanie wykonania decyzji w zakresie dotyczącym administracyjnej kary pieniężnej[502].

Prezesa Urzędu, oprócz uprawnień władczych w postaci wydawania decyzji administracyjnych, przysługują również środki „niewładcze", np. uprawnienie do kierowania tzw. wystąpień. Ich istotą jest podjęcie przez Prezesa Urzędu działań zmierzających do doskonalenia powszechnego systemu ochrony danych. W tym celu organ nadzorczy może zwracać się do różnych podmiotów o podjęcie wskazanych działań. Niewładczy charakter tego rodzaju działań polega na tym, że podmiot, do którego Prezes urzędu skierował wystąpienie nie jest związany treścią wystąpienia. „W piśmiennictwie przedmiotu zwraca się także uwagę na to, że wystąpienie nie jest środkiem w sprawie indywidualnej naruszenia przepisów o ochronie danych osobowych i nie może poprzedzać lub zastępować decyzji nakazowej. Wydanie decyzji nakazowej jest poprzedzone postępowaniem administracyjnym (wg. przepisów K.p.a.). Tym samym w tej samej sprawie organ jednocześnie nie może zastosować wystąpienia oraz wydać nakazu. Prowadziłoby to do niedopuszczalnego dualizmu działań organu"[503]. Jak podkreśla Paweł Fajgielski wnioski te pozostały aktualne na gruncie ustawy z 10 maja 2018 r.[504]

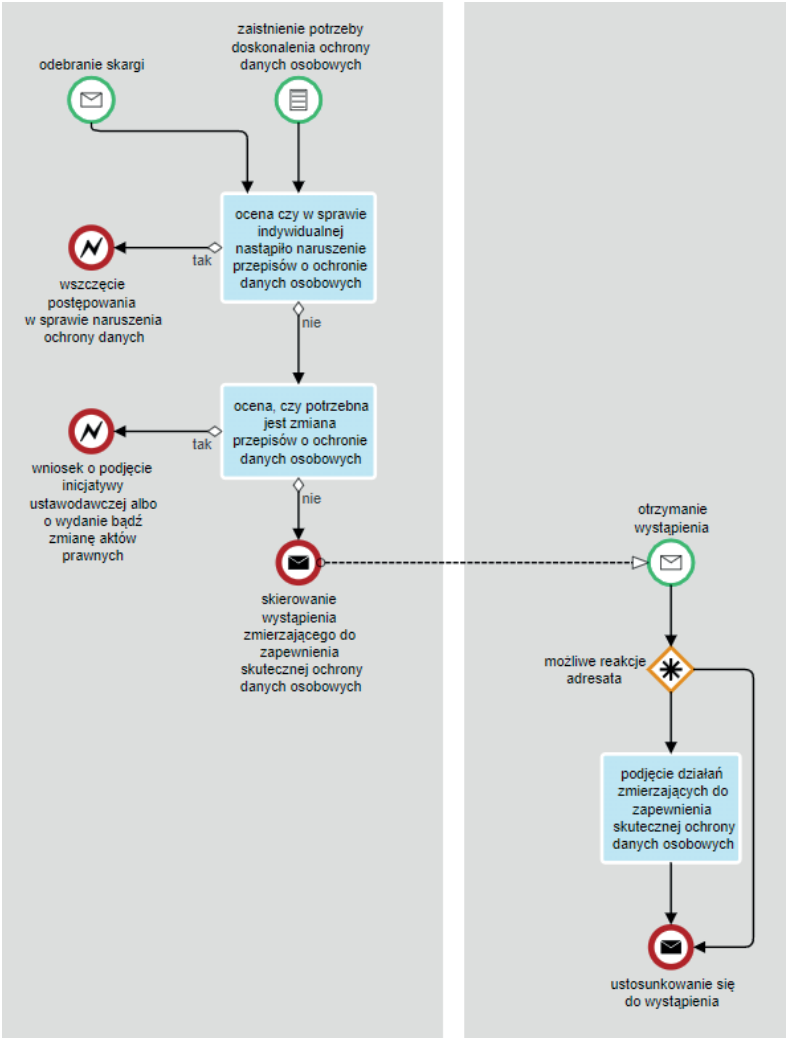
[501] Taki tryb wynika z faktu, że sądy administracyjne kontrolują wyłącznie legalność aktów, podczas gdy w sprawach regulacyjnych istnieje potrzeba kontroli pewnych aspektów pozaprawnych, jak np. kryteria oceny pozycji rynkowej, określenia rynku etc. Szerzej zob. *Aktualne problemy rozgraniczenia właściwości sądów administracyjnych i powszechnych*, red. Błachucki M., Górzyńska T., Naczelny Sąd Administracyjny, Warszawa 2011.

[502] Por. M. Chołodecki, *Model kontroli sądowej decyzji Prezesa Urzędu Komunikacji Elektronicznej*, Internetowy Kwartalnik Antymonopolowy i Regulacyjny 2012, nr 6 (1).

[503] G. Sibiga, *Wystąpienie – nowa kompetencja Generalnego Inspektora Ochrony Danych Osobowych* [w:] *Nowelizacja ustawy o ochronie danych osobowych 2010*, red. G. Sibiga, MoP dodatek specjalny 2011, nr 3, s. 27.

[504] P. Fajgielski, *Prawo ochrony danych osobowych Zarys wykładu*, Wolters Kluwer, Warszawa 2019, s. 182–185.

RYSUNEK 21 Drzewo postępowania w sprawie wystąpienia PUODO



Źródło: P. Fajgielski, *Prawo ochrony danych osobowych Zarys wykładu*, Wolters Kluwer, Warszawa 2019, s. 185

Porównując wcześniejszy stan prawny oraz ten wprowadzony rozporządzeniem 2016/679 można sformułować co najmniej dwie tezy. Po pierwsze w zakresie odpowiedzialności administracyjnej pod rządami nowego systemu prawnego wręcz rewolucyjnie zwiększono wysokość kar administracyjnych. Po drugie uproszczono ścieżkę dojścia do nałożenia kary i jej wysokości. Pod rządami starych przepisów co do zasady aby doszło do nałożenia grzywny trzeba było uparcie „nie przywracać stanu zgodnego z prawem". Warto przy tym zauważyć, że na gruncie starej ustawy GIODO nie mógł od razu nakładać kar finansowych po stwierdzeniu naruszenia przepisów ustawy. Organ wydając decyzję administracyjną, w której stwierdzał naruszenie wymogów

prawnych, wyznaczał adresatowi decyzji termin na usunięcie uchybień. Dopiero w przypadku gdy te uchybienia nie zostały usunięte w wyznaczonym terminie, miał prawo nałożyć karę grzywny. Aktualnie kara jest orzekana już w samej treści decyzji administracyjnej jako sankcja za naruszenie. Grzywny te są nakładane w postępowaniu egzekucyjnym w administracji.

Jak diagnozowano ówcześnie „słabością obecnego systemu ochrony danych osobowych są nieodpowiednie środki (sankcje) zapewniające (czy w niektórych przypadkach wymuszające) stosowanie przepisów o ochronie danych osobowych. (…) Przedsiębiorcy w określonych warunkach podejmują ryzyko nieprzestrzegania przepisów z zakresu ochrony danych osobowych, choćby pozyskując zbiory danych osobowych, np. potencjalnych klientów i nie weryfikując, czy zostały zebrane w sposób legalny lub w sposób nieadekwatny zabezpieczając dane, których są administratorami”[505]. Występowały oczywiście także sankcje wynikające z przepisów karnych, ale rzadko kierowane były zawiadomienia o podejrzeniu popełnienia przestępstwa bądź postępowania były umarzane ze względu na niską szkodliwość społeczną. To była dość wygodna sytuacja dla wielu administratorów danych, którzy nierzadko dochodzili do wniosku, iż korzyści z nieprzestrzegania przepisów z zakresu ochrony danych osobowych są zdecydowanie większe niż negatywne konsekwencje[506].

Sankcje finansowe wprowadzone rozporządzeniem wymusiły refleksję po stronie ich adresatów i stały się istotnym narzędziem gwarantującym poszanowanie przepisów ochrony danych osobowych[507]. Przedsiębiorcy, którzy wcześniej mieli większy apetyt na ryzyko zostali zmuszeni do jego rekalkulacji. W praktyce wysokie kary zmusiły organizacje do przykładania większej wagi do respektowania przepisów ochrony danych osobowych – a co za tym idzie, do inwestowania w bezpieczeństwo i ochronę informacji.

Odpowiedzialność cywilna

Naruszenie prywatności[508], w tym przepisów o ochronie danych osobowych może rodzić odpowiedzialność cywilną. Zgodnie z przepisami rozporządzenia oraz ustawy administrator danych, procesor oraz jakikolwiek sprawca deliktu/szkody w związku z naruszeniem zasad ochrony danych mogą ponieść odpowiedzialność cywilnoprawną.

Do reformy systemu prawnego podstawą odpowiedzialności cywilnoprawnej za naruszenie ochrony danych osobowych w Polsce były – co do zasady – przepisy o ochronie dóbr osobistych (w szczególności art. 23 i 24 k.c.), w związku z przepisami dot. odpowiedzialności deliktowej (i odszkodowawczej)[509], czyli tzw. normy ogólne. I tak choć w art. 23 k.c. dane osobowe nie są wymienione wprost (w wylistowanych enumeratywnie w przepisie przykładach

[505] M. Zadrożny, *Warunki nakładania przez GIODO administracyjnych kar pieniężnych* [w:] *Unijna reforma ochrony danych osobowych. Analiza zmian*, red. A. Dmochowska, M. Zadrożny, Warszawa 2016.
[506] Zob. A. Rogala-Lewicki, *Dane osobowe w systemach państwowych – uprawnienia podmiotowe i sankcje*, Wiedza Prawnicza, Nr 1/2014
[507] Zob. A. Mednis, *Administracyjne kary pieniężne w ogólnym rozporządzeniu i ochronie danych*, Informacja w administracji publicznej 2017, nr 3.
[508] Zob. B. Kordasiewicz, *Cywilnoprawna ochrona prawa do prywatności*, Kwartalnik Prawa Prywatnego 2000, nr 1, s. 19–51. Por. M. Wild, *Ochrona prywatności w prawie cywilnym*, Państwo i Prawo 2001, nr 4, s. 54–72.
[509] Zob. M.Z. Zieliński, *Odpowiedzialność deliktowa pośredniczących dostawców usług internetowych. Analiza prawnoporównawcza*, Wolters Kluwer, Warszawa 2013.

dóbr osobistych), to jednak za odrębną kategorię dobra osobistego, zarówno w doktrynie, jak i w wypracowanym latami orzecznictwie, uznaje się prywatność, a w jej ramach chroniona jest osoba, której dane są przetwarzane. Od 25 maja 2018 roku poszkodowany może (obok norm ogólnych) wprost – formułując roszczenie odszkodowawcze – powołać się na przepisy RODO[510], co jednak nadal nie zmienia zakresu jego ochrony prawnej wynikającej z przepisów prawa cywilnego.

A zatem każda osoba, której prawa przysługujące na mocy przepisów o ochronie danych osobowych zostały naruszone, może żądać zaniechania tego działania, a także może żądać, żeby ten, kto dopuścił się naruszenia, dopełnił czynności potrzebnych do usunięcia jego skutków. Ponadto każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia przepisów rozporządzenia, ma prawo uzyskać od administratora lub podmiotu przetwarzającego odszkodowanie za poniesioną szkodę[511].

Na podstawie tzw. norm ogólnych prawa cywilnego możliwe są trzy podstawy takiej odpowiedzialności: (1) z tytułu naruszenia dóbr osobistych, (2) kontraktowa oraz (3) deliktowa.

Bezprawne działanie „na danych osobowych", np. ujawnienie danych osobowych bez podstawy prawnej może naruszać prywatność osób, których dotyczą[512]. Art. 23 Kodeksu cywilnego zawiera katalog dóbr osobistych chronionych przez prawo cywilne. Zawarty w tym artykule katalog dóbr jest katalogiem otwartym, o czym świadczy zwrot „w szczególności". W kodeksie przyjęto konstrukcję pluralistyczną dóbr osobistych, co oznacza że przedmiotem ochrony są wszelkie, ale jednostkowo wskazane, dobra osobiste, jak zdrowie, wolność, cześć, swoboda sumienia, nazwisko lub pseudonim, wizerunek, tajemnica korespondencji, nietykalność mieszkania, twórczość naukowa, artystyczna, wynalazcza i racjonalizatorska. Pozostają one pod ochroną prawa cywilnego niezależnie od gwarancji przewidzianej w oddzielnych przepisach. Do kategorii dóbr osobistych należy zaliczyć zatem prawo każdego do ochrony danych osobowych, zwłaszcza sensytywnych – materializujące się poprzez stan inkorporowania ochrony danych osobowych w prawie do prywatności.

Katalog roszczeń osoby, której dane zostały naruszone (np. bezprawnie ujawnione) w sytuacjach naruszenia dóbr osobistych obejmuje prawo domagania się od administratora danych osobowych (lub podmiotu przetwarzającego dane) zaniechania zachowania, w wyniku którego ujawnione zostały dane osobowe, przeproszenia lub podjęcia innych czynności mających

[510] Zob. F. Morawski, *Odpowiedzialność cywilna administratora danych osobowych i podmiotu przetwarzającego według ogólnego rozporządzenia o ochronie danych osobowych*, Acta Iuris Stetinensis 2019, Nr 26.

[511] Należy przy tym zwrócić uwagę na pewne rozróżnienie odpowiedzialności administratora oraz podmiotu przetwarzającego. Każdy administrator uczestniczący w przetwarzaniu odpowiada za szkody spowodowane przetwarzaniem naruszającym przepisy RODO, natomiast podmiot przetwarzający odpowiada za szkody spowodowane przetwarzaniem wyłącznie, gdy nie dopełnił obowiązków, które RODO nakłada bezpośrednio na podmioty przetwarzające, lub gdy działał poza zgodnymi z prawem instrukcjami administratora lub wbrew tym instrukcjom. Zarówno administrator, jak i podmiot przetwarzający zostają jednakże zwolnieni z odpowiedzialności, jeżeli udowodnią, że w żaden sposób nie ponoszą winy za zdarzenie, które doprowadziło do powstania szkody. Jeżeli w tym samym przetwarzaniu uczestniczy więcej niż jeden podmiot i zgodnie z RODO odpowiadają oni za szkodę spowodowaną przetwarzaniem, ponoszą oni odpowiedzialność solidarną za całą szkodę, tak by zapewnić osobie, której dane dotyczą, rzeczywiste uzyskanie odszkodowania. Podmiot, który zapłacił odszkodowanie za całą wyrządzoną szkodę, ma prawo żądania od pozostałych podmiotów, które uczestniczyły w tym samym przetwarzaniu, zwrotu części odszkodowania odpowiadającej części szkody, za którą ponoszą odpowiedzialność. T. Mamys, *RODO: Karna i cywilna odpowiedzialność za naruszenie ochrony danych osobowych*, https://www.sage.com/pl-pl/blog/rodo-karna-i-cywilna-odpowiedzialnosc-za-naruszenie-ochrony-danych-osobowych/, [dostęp: 15.12.2020].

[512] W kontekście ochrony prywatności jako wartości konstytucyjnej wpisanej w zasadę demokratycznego państwa prawnego zob. wyrok TK z 24.06.1997, sygn. K 21/96, OTK 1997, nr 2, poz. 23. Por. wyrok TK z 21.10.1998, sygn. K 24/98, OTK 1998, nr 6, poz. 97 (prawo do prywatności – zakres ochronny związany ze sferą życia intymnego oraz sferą życia prywatnego); wyrok TK z 23.06.2009, sygn. K 54/07, OTK-A 2009, nr 6, poz. 86 (ochrona prywatności jako związana z godnością człowieka).

na celu usunięcie skutków ujawnienia danych osobowych. Szczegółowo reguluje tę kwestie przepis art. 24 K.c. Ten, czyje dobro osobiste zostaje zagrożone cudzym działaniem, może żądać zaniechania tego działania, chyba że nie jest ono bezprawne. W razie dokonanego naruszenia może on także żądać, ażeby osoba, która dopuściła się naruszenia, dopełniła czynności potrzebnych do usunięcia jego skutków, w szczególności ażeby złożyła oświadczenie odpowiedniej treści i w odpowiedniej formie. Na zasadach przewidzianych w kodeksie może on również żądać zadośćuczynienia pieniężnego lub zapłaty odpowiedniej sumy pieniężnej na wskazany cel społeczny. Jeżeli wskutek naruszenia dobra osobistego została wyrządzona szkoda majątkowa, poszkodowany może żądać jej naprawienia na zasadach ogólnych.

Z kolei ogólnym przepisem regulującym odpowiedzialność deliktową jest art. 415 Kodeksu cywilnego. Stanowi on, że kto z winy swej wyrządził drugiemu szkodę, obowiązany jest do jej naprawienia. Jeżeli w wyniku niedopełnienia przez administratora danych lub osoby przez niego upoważnionej obowiązków zachowania danych w tajemnicy osoba, której te dane dotyczą poniosła jakąś szkodę na swoim majątku to może ona domagać się jej naprawienia. Ponadto zgodnie z art. 448 K.c. sąd może przyznać temu, czyje dobro zostało naruszone, odpowiednią sumę tytułem zadośćuczynienia pieniężnego za doznaną krzywdę. Na żądanie pokrzywdzonego może też zasądzić odpowiednią sumę pieniężną na wskazany przez niego cel społeczny, niezależnie od innych środków potrzebnych do usunięcia skutków naruszenia.

Szkodę majątkową stanowi uszczerbek w majątku osoby fizycznej, rozumiany zarówno jako rzeczywiście poniesione straty, jak i utracone potencjalne korzyści. Szkoda niemajątkowa oznacza krzywdę, uszczerbek w dobrach niemajątkowych osoby fizycznej (na przykład doznany stres). Administrator lub podmiot przetwarzający dane poniesie odpowiedzialność w przypadku wystąpienia łącznie następujących przesłanek:

- poniesienia przez osobę, której dane dotyczą szkody (majątkowej lub niemajątkowej),
- naruszenia przez administratora lub procesora zasad ochrony danych osobowych (przepisów RODO),
- zaistnienia związku przyczynowo-skutkowego pomiędzy szkodą osoby fizycznej a naruszeniem (zachowaniem wyrażonym działaniem lub zaniechaniem),
- wystąpienia winy po stronie podmiotu dokonującego naruszenia.

Naruszający zatem nie będzie ponosił odpowiedzialności odszkodowawczej jeżeli udowodni, że nie ponosi winy za zdarzenie, które doprowadziło do powstania szkody[513]. Przy czym odpowiedzialność może ponieść nie tylko administrator danych, lecz także podmiot przetwarzający dane osobowe w imieniu administratora, jeżeli działał wbrew instrukcjom przekazanym przez

[513] Administrator danych może bronić się przed roszczeniem powoda, wskazując, że nie ponosi winy za zdarzenie, które skutkowało szkodą po stronie osoby fizycznej. Jeżeli dane osoby fizycznej były wykorzystywane zgodnie z prawem (np. w związku z koniecznością wykonania umowy) i administrator podjął szereg działań zabezpieczających dane przed bezprawnym wykorzystaniem, lecz dane osoby fizycznej zostały wykradzione wskutek ataku hakerskiego, któremu administrator obiektywnie nie był w stanie zapobiec, administrator może bronić się przed żądaniem zapłaty, podnosząc zarzut braku winy. M. Milan, Naruszenie przepisów RODO a odpowiedzialność cywilnoprawna, https://poradnikprzedsiebiorcy.pl/-naruszenie-przepisow-rodo-a-odpowiedzialnosc-cywilnoprawna, [dostęp: 15.12.2020].

administratora danych. Nie mniej odpowiedzialność solidarna tych podmiotów w relacji zewnętrznej sprawia, iż wystarczającym będzie np. skierowanie roszczenia tylko do jednego, wybranego podmiotu, który jest odpowiedzialny za naruszenia, a same roszczenie będzie mogło dotyczyć całej wyrządzonej szkody, a nie tylko części szkody za którą ten podmiot jest faktycznie odpowiedzialny. W stosunkach wewnętrznych nie wyłącza to roszczeń regresowych między tymi podmiotami (można żądać od pozostałych podmiotów zwrotu części odszkodowania w wysokości odpowiadającej części szkody, za którą poniesiono odpowiedzialność).

Ciężar udowodnienia okoliczności przemawiających za zasądzeniem odszkodowania ciąży na powodzie, tj. na osobie fizycznej, która występuje z żądaniem zasądzenia na jej rzecz odszkodowania. W praktyce oznacza to, że powód będzie musiał w toku procesu wnieść dowody wskazujące jednoznacznie, że rzeczywiście doszło do przełamania przepisów o ochronie danych osobowych, naruszenie jest zawinionym czynem administratora danych, a osoba poniosła konkretną szkodę. Biorąc jednakże pod uwagę zasadę rozliczalności, administrator powinien być w stanie wykazać przestrzeganie przez siebie przepisów ochrony danych osobowych. Sprowadzi się to zatem do tego, że ciężar udowodnienia zgodności przetwarzania zostanie przeniesiony na administratora, po przedstawieniu przez podmiot danych dowodów na wystąpienie naruszenia. Administrator lub podmiot przetwarzający zostaną zatem zwolnieni z odpowiedzialności odszkodowawczej, jeżeli udowodnią, że w żaden sposób nie ponoszą winy za zdarzenie, które doprowadziło do powstania szkody. Tym samym *de facto* to na te podmioty przeniesiony został ciężar dowodu, a w konsekwencji osoby, których dane dotyczą, nie będą musiały tej winy wykazywać (art. 82 ust. 3 RODO). Wprost ta kwestia poruszona została w motywie 146 preambuły do rozporządzenia. Za szkodę, którą dana osoba poniosła wskutek przetwarzania w sposób naruszający rozporządzenie, powinno przysługiwać odszkodowanie od administratora lub podmiotu przetwarzającego. Administrator lub podmiot przetwarzający powinni jednak zostać zwolnieni z odpowiedzialności prawnej, jeżeli udowodnią, że szkoda w żadnym razie nie powstała z ich winy[514]. Pojęcie szkody należy interpretować szeroko, w świetle orzecznictwa Trybunału Sprawiedliwości, w sposób w pełni odzwierciedlający cele rozporządzenia. Nie ma to wpływu na roszczenia z tytułu szkód wynikających z naruszenia innych przepisów prawa Unii lub prawa państwa członkowskiego. Przetwarzanie dokonywane w sposób naruszający rozporządzenie obejmuje także przetwarzanie, które narusza akty delegowane i wykonawcze przyjęte na mocy rozporządzenia oraz prawo państwa członkowskiego doprecyzowujące rozporządzenie. Osoby, których dane dotyczą, powinny uzyskać pełne i skuteczne odszkodowanie za poniesione szkody. Jeżeli administratorzy lub podmioty przetwarzające uczestniczą w tym samym przetwarzaniu, każdy administrator lub podmiot przetwarzający powinien odpowiadać prawnie za całość szkody. Jeżeli jednak zostaną włączeni do jednego postępowania sądowego zgodnie z prawem państwa członkowskiego, odszkodowaniem można obarczyć każdego z administratorów i każdy

[514] Motyw 146 preambuły 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 (Dz. Urz. UE L 119 z dn. 4.05.2016, s. 1–88).

z podmiotów przetwarzających stosownie do ich winy za szkodę wynikłą z przetwarzania, o ile osobie, której dane dotyczą, zapewnione zostanie pełne i skuteczne odszkodowanie za poniesioną szkodę. Każdy administrator lub podmiot przetwarzający, który wypłacił pełne odszkodowanie, może następnie dochodzić roszczeń regresowych wobec innych administratorów lub podmiotów przetwarzających uczestniczących w tym samym przetwarzaniu.

Prawo do odszkodowania (przesłanka lex specialis)

Przepisy RODO przyznają każdej osobie fizycznej, której dobra zostały naruszone, prawo do wystąpienia z samodzielnym roszczeniem o zapłatę odszkodowania za naruszenie przepisów ochrony danych osobowych. Począwszy od 25 maja 2018 r. ogólne podstawy wynikające z prawa cywilnego uległy poszerzeniu o możliwość bezpośredniego powołania się na przepisy unijne dotyczące odpowiedzialności odszkodowawczej za naruszenie zasad ochrony danych osobowych, a ponadto na uzupełniające regulacje rozporządzenia, przepisy nowej ustawy o ochronie danych osobowych. Wprowadzono nową podstawę dochodzenia roszczeń cywilnoprawnych w postaci art. 82 RODO, który w swojej treści stanowi, że każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia rozporządzenia, ma prawo uzyskać odszkodowanie za poniesioną szkodę od administratora lub podmiotu przetwarzającego.

Oprócz wyżej wymienionej podstawy prawnej, za przesłankę odpowiedzialności cywilnoprawnej uznaje się również przepis art. 79 ust. 1 rozporządzenia, który zapewnia prawo podmiotu danych osobowych do skutecznego środka ochrony prawnej przed sądem, jeżeli ten uzna, że prawa przysługujące jej na mocy rozporządzenia zostały naruszone w wyniku przetwarzania jego danych osobowych z naruszeniem rozporządzenia. Stąd przyjmuje się, że art. 79 ust. 1 obejmuje zarówno środki o charakterze materialnoprawnym jak i procesowym[515].

Podstawą żądania będzie zatem przepis art. 82 ust. 1, art. 79 ust. 1 RODO w związku z przepisem art. 92 ustawy o ochronie danych osobowych, który stanowi jak następuje.

1) każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia rozporządzenia, ma prawo uzyskać od administratora lub podmiotu przetwarzającego odszkodowanie za poniesioną szkodę.
2) każdy administrator uczestniczący w przetwarzaniu odpowiada za szkody spowodowane przetwarzaniem naruszającym rozporządzenie. Podmiot przetwarzający odpowiada za szkody spowodowane przetwarzaniem wyłącznie, gdy nie dopełnił obowiązków, które rozporządzenie nakłada bezpośrednio na podmioty przetwarzające, lub gdy działał poza zgodnymi z prawem instrukcjami administratora lub wbrew tym instrukcjom.

[515] Wątpliwość dotyczy natomiast tego czy wymaga on wprowadzenia dodatkowych przepisów do polskiego porządku prawnego. Można bowiem argumentować, że w polskim systemie prawnym istnieją skuteczne środki ochrony prawnej przed sądem, w przypadku gdy podmiot danych uzna, że prawa przysługujące mu na mocy RODO zostały naruszone w wyniku przetwarzania jego danych osobowych z naruszeniem rozporządzenia. Są nimi właśnie przepisy o ochronie dóbr osobistych. Wątpliwości te zostały wprost rozstrzygnięte w projekcie ustawy o ochronie danych osobowych, którego rozdział 8 (art. 78–81) poświęcono odpowiedzialności cywilnej za naruszenie przepisów o ochronie danych osobowych. Na mocy projektowanego art. 78 ust. 1 każda osoba, której prawa przysługujące na mocy przepisów o ochronie danych osobowych zostały naruszone, będzie mogła żądać zaniechania tego działania, a także może żądać, ażeby ten, kto dopuścił się naruszenia, dopełnił czynności potrzebnych do usunięcia jego skutków. W art. 78 ust. 2 – 3 projektu ustawy przesądzono, że dochodzenie roszczeń w oparciu o art. 78 projektu nie wyłącza możliwości wystąpienia z innymi roszczeniami z tytułu naruszenia przepisów o ochronie danych osobowych. Chodzi zarówno o możliwość powołania art. 82 RODO, jak i obecnych przepisów o ochronie dóbr osobistych.

Zgodnie z postanowieniami motywu 146, przetwarzanie dokonywane w sposób naruszający RODO obejmuje także przetwarzanie, które narusza akty delegowane i wykonawcze przyjęte na jego mocy oraz prawo państwa członkowskiego je doprecyzowujące. Tym samym, szkoda podmiotu danych może być spowodowana nie tylko niezgodnością postępowania z zasadami przetwarzania wskazanymi w RODO, ale również m.in. w ustawie o ochronie danych osobowych, bądź ustawie o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia. Warto przy tym pamiętać, że ostatnia z powołanych ustaw wprowadza zmiany w wielu przepisach sektorowych takich jak np. Kodeks Pracy czy Prawo bankowe.

Postępowanie w sprawie zasądzenia roszczeń odszkodowawczych dochodzonych na podstawie art. 82 ust. 1 rozporządzenia za poniesioną przez osobę fizyczną szkodę majątkową lub niemajątkową toczy się w oparciu o przepisy Kodeksu postępowania cywilnego, z uwzględnieniem szczególnych regulacji przewidzianych w ustawie o ochronie danych osobowych w rozdziale 10 (art. 100 ustawy)[516]. Sądem właściwym do rozpoznania tego typu spraw – niezależnie od wartości przedmiotu sporu – jest sąd okręgowy (art. 93 ustawy). Ustawa nie przewiduje żadnych szczególnych regulacji dotyczących właściwości miejscowej sądu, a zatem należy uznać, że będzie to sąd właściwości ogólnej pozwanego[517].

Ustawa o ochronie danych osobowych przewiduje określone kompetencje dla Prezesa Urzędu. W szczególności organ ten, w sprawach o roszczenia z tytułu naruszenia przepisów o ochronie danych osobowych, ma prawo do wytaczania powództw na rzecz osoby fizycznej, której dane dotyczą. Prezes UODO może, za zgodą powoda, przystąpić do już toczącego się postępowania, w każdy jego stadium, chyba że toczy się przed nim postępowanie dotyczące tego samego naruszenia przepisów o ochronie danych osobowych (art. 98 ustawy). Prezes UODO jeżeli uzna, że przemawia za tym interes publiczny, ma prawo do przedstawienia sądowi rozpoznającemu sprawę istotnego poglądu w sprawie (art. 99 ustawy). Ponadto ustawa przewiduje obowiązek wymiany informacji między sądem a Prezesem Urzędu, w tym:

- powiadomienia Prezesa UODO o wniesieniu pozwu oraz o prawomocnym zakończeniu sprawy (art. 94 ust. 1 ustawy),
- poinformowaniu sądu (w sytuacji powzięcia informacji przez Prezesa Urzędu toczącym się postępowaniu) o każdej sprawie dotyczącej tego samego naruszenia przepisów o ochronie danych osobowych, która toczy się przed Prezesem Urzędu lub sądem administracyjnym albo została zakończona, przy jednoczesnym obowiązku Prezesa Urzędu do niezwłocznego informowania sądu również o wszczęciu każdego postępowania w sprawie dotyczącej tego samego naruszenia (art. 94 ust. 2 ustawy).

[516] Szerzej zob. G. Sibiga, *Postępowanie w sprawach ochrony danych osobowych*, Dom Wydawniczy ABC, Warszawa 2003.

[517] Na temat rozgraniczenia postępowań z zakresu kwestionowania nałożonych kar administracyjnych (sądy administracyjne) oraz pozostałych roszczeń (sądy cywilne) zob. *Aktualne problemy rozgraniczenia właściwości sądów administracyjnych i powszechnych*, red. Błachucki M., Górzyńska T., Naczelny Sąd Administracyjny, Warszawa 2011.

Sąd zawiesza postępowanie, jeżeli sprawa dotycząca tego samego naruszenia przepisów o ochronie danych osobowych została wszczęta przed Prezesem Urzędu (art. 95 ustawy).

Ustalenia poczynione w treści prawomocnej decyzji Prezesa UODO o stwierdzeniu naruszenia przepisów o ochronie danych osobowych lub w prawomocnym wyroku sądu administracyjnego wiążą sąd cywilny w postępowaniu o naprawienie szkody wyrządzonej przez naruszenie przepisów RODO w zakresie stwierdzenia naruszenia tych przepisów[518]. Jeżeli roszczenie powoda zostało już rozpoznane przez Prezesa UODO (albo sąd administracyjny w związku z postępowaniem skargowym), sąd umorzy postępowanie wszczęte pozwem – lecz tylko wówczas, gdy w postępowaniu administracyjnym roszczenie powoda zostało uwzględnione (art. 96 ustawy[519]).

Oczywiście wystąpienie z roszczeniem odszkodowawczym, nie wyłącza możliwości wystąpienia z innymi roszczeniami z tytułu naruszenia przepisów o ochronie danych osobowych. Na gruncie nieuregulowanym przepisami rozporządzenia lub ustawy zastosowanie znajdą przepisy polskiego Kodeksu cywilnego (art. 92 ustawy).

Odpowiedzialność cywilna oraz prawo do żądania odszkodowania oparte o *lex specialis* (art. 82 RODO) ma zatem charakter niezależny od innych możliwych sankcji przewidzianych w rozporządzeniu oraz ustawie o ochronie danych osobowych. A zatem za całkowicie prawdopodobne uznać należy sytuację, w której wobec podmiotu który naruszył RODO, Prezes Urzędu nałoży administracyjną karę pieniężną, a poza tym roszczenia o odszkodowanie skierują wobec administratora lub procesora osoby, których dane były przetwarzane niezgodnie z wymaganiami RODO. Obok tego pojawia się również odpowiedzialność karnoprawna.

Odpowiedzialność karna

O ile kary administracyjne – w swojej charakterystyce – są przede wszystkim adresowane do osób prawnych, to przepisy karne mają zastosowanie do osób fizycznych. O możliwości wprowadzania sankcji karnych w ustawodawstwach państw członkowskich stanowi punkt 149 preambuły do RODO. Państwa członkowskie powinny mieć możliwość ustanawiania przepisów przewidujących sankcje karne za naruszenie rozporządzenia, w tym za naruszenie krajowych przepisów przyjętych na jego mocy i w jego granicach[520]. Sankcje karne mogą również obejmować pozbawienie zysków wynikających z naruszenia rozporządzenia. Jednak nałożenie sankcji karnych za naruszenie takich krajowych przepisów oraz nałożenie sankcji administracyjnych nie powinno prowadzić do naruszenia zasady *ne bis in idem*, zgodnie z wykładnią Trybunału Sprawiedliwości[521].

[518] Ustalenia prawomocnej decyzji Prezesa Urzędu o stwierdzeniu naruszenia przepisów o ochronie danych osobowych lub prawomocnego wyroku wydanego w wyniku wniesienia skargi, o której mowa w art. 145a § 3 ustawy z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi, wiążą sąd w postępowaniu o naprawienie szkody wyrządzonej przez naruszenie przepisów o ochronie danych osobowych co do stwierdzenia naruszenia tych przepisów.

[519] Sąd umarza postępowanie w zakresie, w jakim prawomocna decyzja Prezesa Urzędu o stwierdzeniu naruszenia przepisów o ochronie danych osobowych lub prawomocny wyrok wydany w wyniku wniesienia skargi, o której mowa w art. 145a § 3 ustawy z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi, uwzględnia roszczenie dochodzone przed sądem.

[520] Zob. 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.

[521] M. Zimna, *Odpowiedzialność karna za naruszenie ochrony danych osobowych*, Prokuratura i Prawo 2020, nr 1, s. 73.

Do 2018 roku, pod rządami dyrektywy 95/46/WE, na państwa członkowskie nałożone zostało zobowiązanie do przyjęcia „odpowiednich środków" celem zapewnienia pełnej realizacji postanowień dyrektywy. W szczególności, państwa członkowskie zostały zobowiązane do określenia katalogu sankcji, które mogą zostać nałożone w przypadku naruszenia postanowień ww. dyrektywy. Przepisy tego aktu nie precyzowały natomiast, jakiego rodzaju środki ochrony prawnej miałyby zostać wprowadzone w ustawodawstwach państw członkowskich. W wykonaniu zobowiązania określonego w art. 24 dyrektywy, w przepisach ustawy o ochronie danych osobowych z 1997 roku ustanowiony został system przepisów karnych. System ten zakładał wyznaczenie ośmiu (uwzględniając typy uprzywilejowane i typ kwalifikowany), pozakodeksowych (zewnętrznych wobec Kodeksu karnego) typów czynów zabronionych, z których każdy miał charakter występku ściganego z urzędu, z oskarżenia publicznego[522]. Otóż za naruszenie przepisów ochrony danych osobowych groziła ówcześnie odpowiedzialność przewidziana w następujących normach karnych:

- za przetwarzanie danych osobowych bez podstawy prawnej – ograniczenie lub pozbawienie wolności do 2 lat (art. 49 K.k.)[523],
- za udostępnienie lub umożliwienie dostępu do danych osobom nieupoważnionym – ograniczenie lub pozbawienie wolności do 2 lat (art. 51 K.k.),
- za niezabezpieczenie danych w odpowiedni sposób przed zabraniem, uszkodzeniem lub zniszczeniem przez osobę nieuprawnioną – ograniczenie lub pozbawienie wolności do roku (art. 52 K.k.),
- za niezgłoszenie zbioru danych do rejestracji – ograniczenie lub pozbawienie wolności do 2 lat (art. 53 K.k.),
- za niedopełnienie obowiązku poinformowania osoby, której dane dotyczą, o jej prawach, lub nieprzekazanie tej osobie informacji umożliwiających korzystanie z praw przyznanych jej w ustawie – ograniczenie lub pozbawienie wolności do roku (art. 54 K.k.),
- za udaremnianie lub utrudnianie wykonania czynności kontrolnej – ograniczenie lub pozbawienie wolności do 2 lat (art. 54a K.k.).

Konstrukcja przepisów karnych wskazywała, iż ich głównym adresatem były osoby posiadające status administratora danych. Czyn bowiem mogły popełnić co do zasady osoby zarządzające jednostką organizacyjną. Wyjątkiem były przepisy art. 51 i 54a ustawy, za których naruszenie ponosić odpowiedzialność mógł także inny podmiot, np. pracownik[524].

[522] Zob. B. Kurzępa, *Przestępstwa z ustawy o ochronie danych osobowych*, Prokuratura i Prawo 1999, nr 6.

[523] Artykuł 49 ust. 2 ustawy o ochronie danych osobowych stanowi, że jeżeli czyn z art. 49 ust. 1 dotyczy danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3. Ze względu na charakter danych o stanie zdrowia nielegalne ich przetwarzanie wypełnia znamiona przestępstwa z art. 49 ust. 2 ustawy o ochronie danych osobowych, który przewiduje typ kwalifikowany. Sprawcą przestępstwa z art. 49 ustawy o ochronie danych osobowych może być każdy – gdy chodzi o niedozwolone przetwarzanie danych, oraz osoba, która nie jest uprawniona do ich przetwarzania – w zakresie przetwarzania danych bez uprawnienia. W tym drugim wypadku chodzi o każdego z wyjątkiem osoby upoważnionej zgodnie z art. 31 i 35 ustawy o ochronie danych osobowych. Omawiane przestępstwo może być popełnione w dwojaki sposób: poprzez przetwarzanie danych w wypadkach, gdy jest to niedopuszczalne oraz poprzez przetwarzanie danych, które wprawdzie jest dopuszczalne, ale dokonuje tego osoba nieuprawniona.

[524] Zob. R. Hamm, *Ochrona danych a prawo karne* [w:] O*chrona danych osobowych*, red. M. Wyrzykowski, Instytut Spraw Publicznych, Warszawa 1999, s. 73–88.

Uznaje się, że system sankcji karnych panujący w Polsce do 2018 roku był iluzoryczny[525]. Sankcje administracyjne były nieproporcjonalnie niskie w porównaniu do potencjalnych rozmiarów szkód.[526]. W doktrynie (w tym wśród autorów komentarzy do ustawy z 1997 roku), jak również wśród praktyków, panowało powszechne przekonanie, że system przepisów karnych zawartych w rozdziale 8 ustawy o ochronie danych osobowych jest mało efektywny jako narzędzie służące do zapewnienia przestrzegania przepisów o ochronie danych osobowych[527]. Akcentowano, że „iluzoryczność ochrony wynika m.in. z konstrukcji przestępstw stypizowanych w art. 53 i 54 ustawy jako typów wyłącznie umyślnych, czy też z ograniczenia stosowania art. 49 ust. 1 i 2 ustawy do działania na zbiorze danych osobowych. Jednocześnie uznanie zachowań, takich jak niezgłoszenie zbioru danych osobowych do rejestracji czy naruszenie obowiązków informacyjnych względem osób, których dane dotyczą, wydaje się z perspektywy zawartości bezprawia takiego zachowania oraz jego społecznej szkodliwości nieuzasadnioną kryminalizacją zachowań, które nie powinny być uznane za przestępcze”[528]. Ilustrację niewielkiej efektywności przepisów karnych, jako narzędzia służącego zapewnieniu przestrzegania zasad ochrony danych osobowych, stanowią dane statystyczne dotyczące liczby prawomocnych skazań w poszczególnych latach obowiązywania ustawy.

TABELA 17 Prawomocne skazania w latach 2001-2014 za poszczególne przestępstwa określone w ustawie o ochronie danych osobowych z 1997 roku – zestawienie danych

	2001 r.	2002 r.	2003 r.	2004 r.	2005 r.	2006 r.	2007 r.
Art. 49 ust. 1	–	3	1	8	1	7	2
Art. 49 ust. 2	1	–	–	1	1	1	–
Art. 50	1	–	–	–	–	1	–
Art. 51 ust. 1	6	2	5	13	10	16	11
Art. 51 ust. 2	1	1	2	4	1	3	2
Art. 52	1	5	1	7	10	4	7
Art. 53	–	–	–	1	1	–	–
Art. 54	–	1	–	1	1	–	–

	2008 r.	2009 r.	2010 r.	2011 r.	2012 r.	2013 r.	2014 r.
Art. 49 ust. 1	2	5	7	4	3	1	–
Art. 49 ust. 2	–	1	1	–	–	–	1
Art. 50	–	–	–	–	–	–	1
Art. 51 ust. 1	10	7	8	12	7	2	6
Art. 51 ust. 2	3	1	2	4	3	1	1
Art. 52	7	3	1	9	2	5	11
Art. 53	–	2	3	–	–	–	–
Art. 54	–	–	–	1	–	–	–

Źródło: K. Buczkowski, *Prawnokarna problematyka ochrony danych osobowych*, Instytut Wymiaru Sprawiedliwości, Warszawa 2015, s. 44–49

[525] Stan ten próbowano zmienić przedstawionym przez Prezydenta Rzeczypospolitej Polskiej projektem ustawy o zmianie ustawy o ochronie danych (Sejm VI kadencji, druk sejmowy Nr 488). Autorzy projektu proponowali wyposażenie GIODO w kompetencję do nakładania w drodze decyzji administracyjnych kar pieniężnych. Kary miały być nakładane w wysokości stanowiącej równowartość w złotych polskich od 1000 do 100 000 euro. Co istotne, przesłanką nałożenia kary nie byłoby naruszenie przepisów o ochronie danych osobowych, ale niewykonanie prawomocnej decyzji administracyjnej GIODO. W wyniku prac sejmowych, pierwotna propozycja została jednak zarzucona, a w jej miejsce poddano decyzje administracyjne GIODO egzekucji w trybie egzekucji w administracji. Zob. K. Buczkowski, *Prawnokarna problematyka ochrony danych osobowych*, Warszawa 2015, s. 3, https://iws.gov.pl/wp-content/uploads/2018/08/IWS_Buczkowski-K._Prawnokarna-problematyka-ochrony-danych-osobowych.pdf, [dostęp: 07.12.2020]. Por. S. Hoc, *Karnoprawna ochrona informacji*, Studia i Monografie Uniwersytet Opolski 2012, nr 481.

[526] Tymczasem na tle rozwiązań funkcjonujących w innych państwach UE należy stwierdzić, że już na podstawie dyrektywy 95/46/WE państwa UE wprowadzały rozwiązanie oparte wyłącznie o system kar pieniężnych – bez przepisów karnych (rozwiązanie stosowanie m.in. w Czechach na mocy ustawy z 4 kwietnia 2000r., na Słowacji na mocy ustawy ustawa 428/2002, w Finlandii na mocy ustawy 523/1999, na Malcie na mocy ustawy XXVI/2001) bądź też obok norm karnoprawnych (np. w Portugalii na mocy ustawy z 26 października 1998 r., czy w Holandii na mocy ustawy z 3 lipca2000r.). Zob. B. Fischer, *Przestępstwa komputerowe i ochrona informacji*, Państwo i Prawo 2001, nr 1.

[527] Zob. A. Zoll, *Ochrona prywatności w prawie karnym*, Czasopismo Prawa Karnego 2000, nr 1.

[528] P. Barta, P. Litwiński. *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2013, s. 439.

W okresie objętym statystykami (lata 2011–2014), spośród wszystkich prawomocnych skazań nie została orzeczona ani jedna kara pozbawienia wolności bez zawieszenia. Kary pozbawienia wolności w zawieszeniu stanowiły 18,5% orzekanych kar, kary ograniczenia wolności 12,9%, a w pozostałym zakresie orzekane były kary grzywny. Spośród kar grzywny, w analizowanym okresie nie została orzeczona żadna kara grzywny w wysokości przekraczającej 5000 zł.[529].

Wymierzanie sankcji za naruszenie przepisów o ochronie danych osobowych byłoby realizowane w stopniu znacznie skuteczniejszym, gdyby naruszenia przepisów ustawy z 1997 roku mogły ówcześnie uruchamiać procedurę nałożenia kary o charakterze pieniężnym (co stanowiło nierzadko postulat *de lege ferenda*)[530].

Porównując rozwiązania zaproponowane w aktualnie obowiązującej ustawie o ochronie danych osobowych z konstrukcją odpowiedzialności karnej obowiązującą w rozdziale 8 ustawy z 1997 roku warto nadto zauważyć, że nastąpiła redukcja – pod względem ilościowym – typów przestępstw. Od wejścia w życie RODO prawodawca unijny w zakresie odpowiedzialności karnej pozostawił państwom członkowskim sporą swobodę. Zastrzegł jednak, że sankcje karne muszą być skuteczne, proporcjonalne i odstraszające (art. 84 ust. 1 zd. 2 RODO), przy czym granice zgodnego z prawem przetwarzania danych osobowych, w myśl regulacji konstytucyjnych, powinny zostać określone w aktach ustawowych. Z tej możliwości skorzystał polski ustawodawca, wprowadzając w ustawie z dnia 10 maja 2018 r. normy karnoprawne. Jeszcze na etapie uzasadnienia do projektu ustawy normodawca wskazywał, iż odpowiedzialność karna powinna odnosić się do najpoważniejszych naruszeń przepisów. Odpowiedzialność karna miała być co do zasady wyjątkiem przewidzianym dla najcięższych naruszeń przepisów i stanowić jedynie uzupełnienie dla odpowiedzialności administracyjnej oraz cywilnej[531].

Czynem zabronionym wskazanym w ustawie z 2018 roku jest bezprawne przetwarzanie danych osobowych[532]. Przepis stanowi, iż kto przetwarza dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do ich przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch (art. 107 ust. 1. ustawy)[533]. Oznacza to, że przestępstwo bezprawnego przetwarzania danych może być popełnione w dwóch przypadkach: (1) gdy przetwarzanie danych osobowych nie było dopuszczalne, albo gdy (2) przetwarzanie danych osobowych miało miejsce przez osobę, która nie była do tego

[529] K. Buczkowski, *Prawnokarna problematyka ochrony danych osobowych*, Instytut Wymiaru Sprawiedliwości, Warszawa 2015, s. 44–49.
[530] Zob. W. Kulesza, *Ochrona danych osobowych a nowa kodyfikacja prawa karnego w Polsce* [w:] *Ochrona danych osobowych*, red. M. Wyrzykowski, Instytut Spraw Publicznych, Warszawa 1999, s. 89–97.
[531] G. Szpor, *Publicznoprawna ochrona danych osobowych*, PUG 1999, nr 12, s. 4.
[532] Por. A. Wolska-Bagińska, *Podstawy prawne przetwarzania danych osobowych w postępowaniu karnym*, Prokuratura i Prawo 2018, nr 6.
[533] Przepis art.4 RODO zawiera definicje terminów relewantnych dla przypisania odpowiedzialności. I tak „dane osobowe" oznaczają 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. Natomiast „przetwarzanie" oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak 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. Zob. 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.

uprawniona. W kontekście pierwszej przesłanki z niedopuszczalnością przetwarzania danych mamy do czynienia w sytuacji:

1) gdy nie zachodzi żadna z przesłanek zgodności przetwarzania danych z prawem, określonych w art. 6 i 10 RODO lub/oraz
2) gdy podmiot wyraził skuteczny sprzeciw wobec przetwarzania danych (art. 21 RODO).

Z kolei przetwarzanie przez osobę nieuprawnioną zachodzi wówczas, gdy osoba przetwarzająca nie jest uprawniona do tego typu działań (np. nie ma stosownego upoważnienia wystawionego przez administratora danych).

Ustawodawca wprowadza też kwalifikowaną formę przestępstwa. W sytuacji gdy czyn zabroniony jest popełniony na danych wrażliwych (sensytywnych) w rozumieniu RODO, tj. danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, danych genetycznych, danych biometrycznych przetwarzanych w celu jednoznacznego zidentyfikowania osoby fizycznej, danych dotyczących zdrowia, seksualności lub orientacji seksualnej, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat trzech (art. 107 ust. 2 ustawy) – co oznacza, iż górny limit kary wynosi 3 lata bezwzględnego pozbawienia wolności.

Odpowiedzialność karną ponoszą zawsze oznaczone osoby fizyczne, którym ta odpowiedzialność może zostać przypisana, zgodnie z zasadami prawa karnego materialnego i procesowego. Naruszenie przepisów o ochronie danych osobowych stanowi czyn zabroniony w rozumieniu przepisów Kodeksu karnego. Orzekanie w sprawach karnych dotyczących naruszeń ochrony danych osobowych oczywiście następuje na podstawie przepisów Kodeksu postępowania karnego[534]. Stąd aktualne pozostaje dorobek orzeczniczy sądów karnych[535]. W przypadku popełnienia przestępstwa przez osobę fizyczną związaną z tzw. podmiotem zbiorowym w rozumieniu art. 2 ustawy z 28 października 2002 roku o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary, podmiot ten nie poniesie odpowiedzialności na zasadach określonych w ustawie, ze względu na nieobjęcie przepisów karnych komentowanej ustawy odpowiedzialnością podmiotów zbiorowych (art. 16 ww. ustawy).

Przestępstwa określone w art. 107 ustawy są ścigane z urzędu. Bezprawne przetwarzanie danych stanowi występek (górna granica kary nie przekracza 3 lat), który można popełnić tylko umyślnie. Charakter przestępstwa jest formalny, odpowiedzialność karna nie zależy od wystąpienia skutku. Wystarczy, że zaistnieje sama czynność przetwarzania. Odpowiedzialności karnej podlega nie tylko sprawca (w tym sprawca kierowniczy lub polecający) i współsprawca przestępstwa, ale także podżegacz i pomocnik (art. 18 k.k.). Odpowiedzialność obejmuje również usiłowanie (art. 13 k.k.).

[534] W zakresie postępowania dowodowego szerzej zob. m.in. 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.

[535] Przykładowo na temat zachowania materiałów zebranych w toku kontroli operacyjnej prowadzonej bez zgody sądu oraz legalności i zasadności wydanego przez prokuratora zezwolenia na ujawnienie danych osobowych i wizerunku osób, przeciwko którym toczy się postępowanie przygotowawcze zob. wyrok TK z 12.12.2005, sygn. K 32/04, OTK-A 2005, nr 11, poz. 132, oraz wyrok TK z 18.07.2011, sygn. K 25/09, OTK-A 2011, nr 6, poz. 57.

Równolegle ustawodawca wprowadził odpowiedzialność karną za zachowania mające na celu udaremnienie lub utrudnienie prowadzenia kontroli prowadzonej w ramach postępowania kontrolnego, które w Polsce przeprowadza Prezes Urzędu Ochrony Danych Osobowych. Zgodnie z art. 108 ustawy kto udaremnia lub utrudnia kontrolującemu prowadzenie kontroli przestrzegania przepisów o ochronie danych osobowych, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch. Udaremnienie kontroli lub jej utrudnianie może w szczególności polegać m.in. na niewpuszczeniu na dany teren osób zamierzających przeprowadzić kontrolę, zniszczeniu, ukryciu, uszkodzeniu, usunięciu lub uczynieniu bezużytecznym dokumentów, które kontrolujący mają zbadać, uniemożliwieniu pobrania próbek jak również niedopuszczaniu do pewnych materiałów, urządzeń lub pomieszczenia, udzielaniu nieprawdziwych informacji lub też odmowie udzielania informacji. Niezależnie od tego, czy w czynności kontrolne została zaangażowana policja, osoba utrudniająca przeprowadzenie kontroli będzie podlegała odpowiedzialności karnej[536]. Przestępstwo określone w art. 108 ustawy jest ścigane z urzędu i stanowi występek, który można popełnić tylko umyślnie. Przestępstwo ma charakter powszechny, może je popełnić każdy, kto udaremnia lub utrudnia kontrolującemu prowadzenie kontroli przestrzegania przepisów o ochronie danych osobowych. Odpowiedzialności karnej podlega nie tylko sprawca i współsprawca, ale także podżegacz lub pomocnik, a odpowiedzialność obejmuje także usiłowanie. Jest to przestępstwo materialne, zatem może zostać popełnione również przez zaniechanie (art. 2 k.k.).

Taka konstrukcja występku implikuje oczywiste przypuszczenie, że jego popełnienie będzie – co do zasady – możliwe wyłącznie przez osobę wykonującą funkcję administratora danych lub osoby podległe (pracownicy i inne osoby przetwarzające dane u administratora). Stąd aktualny jest pogląd, że zachowanie osób postronnych może doprowadzić do udaremnienia lub utrudnienia wykonania czynności kontrolnej ale osobom takim trudno będzie wykazać umyślność ich zachowania. Tym samym trudno będzie też przypisać winę lub wykazać formę pomocnictwa, jeżeli działanie osób postronnych było nieumyślne[537].

Wyżej przywołane dwa przepisy wyczerpują katalog sankcji przewidzianych samą ustawą o ochronie danych osobowych[538]. Obok przestępstw regulowanych w akcie specjalnie dedykowanym ochronie danych osobowych, polskie przepisy przewidują odpowiedzialność karną za czyny popełnione „na danych osobowych", a wprowadzone również w innych

[536] M. Jachimowicz, *Przestępstwo zakłócenia kontroli (art. 225 k.k.)*, Prokuratura i Prawo 2008, nr 7–8, s. 42.

[537] A. Dmochowska, M. Zadrożny, *Unijna reforma ochrony danych osobowych. Analiza zmian*, Warszawa 2016, s. 153.

[538] Pierwotna wersja przepisów karnych brzmiała następująco. Kto udaremnia lub utrudnia kontrolującemu prowadzenie kontroli przestrzegania przepisów o ochronie danych osobowych, podlega grzywnie. (orzekanie w sprawach o te czyny miało następować w trybie przepisów Kodeksu postępowania w sprawach o wykroczenia) Kto bez podstawy prawnej przetwarza dane, o których mowa w art. 9 rozporządzenia 2016/679, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku (orzekanie w sprawach o te czyny miało następować w trybie przepisów Kodeksu postępowania karnego. Nastąpiło zatem (na etapie prac nad ustawą) znaczne rozszerzenie przepisów karnych. W poprzednim projekcie kara pozbawienia wolności do 1 roku groziła jedynie za przetwarzanie szczególnych kategorii danych bez podstawy prawnej. W nowym projekcie objęto przepisami karnymi zarówno przetwarzanie danych zwykłych (do 2 lat), jak i znacznie zwiększono karę za przetwarzanie danych wrażliwych (z 1 do 3 lat). Ponadto ustanowiono karę pozbawienia wolności do lat 2 za utrudnianie wykonywania kontroli Prezesowi Urzędu. Ponadto w odniesieniu do kary za przetwarzanie danych wrażliwych zmniejszono precyzyjność przepisu, który w poprzedniej wersji był dużo bardziej dookreślony. Obecnie jest mowa o przetwarzaniu niedopuszczalnym lub takim, do którego nie jest się uprawnionym a nie o braku podstawy. Zob. *Omówienie projektu ustawy o ochronie danych osobowych*, GDPR.PL, https://gdpr.pl/omowienie-projektu-ustawy-o-ochronie-danych-osobowych, [dostęp: 02.12.2020]. Por. Projekt ustawy o ochronie danych osobowych skierowany na Komitet do Spraw Europejskich Rady Ministrów, https://www.gov.pl/web/cyfryzacja/projekt-ustawy-o-ochronie-danych-osobowych-skierowany-na-komitet-do-spraw-europejskich-rady-ministrow, [dostęp: 02.12.2020].

aktach prawnych. I tak ustawa o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, będącą implementacją dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680[539] (tzw. ustawa DODO), określa zasady i warunki ochrony danych osobowych przetwarzanych przez właściwe organy w celu rozpoznawania, zapobiegania, wykrywania i zwalczania czynów zabronionych, w tym zagrożeń dla bezpieczeństwa i porządku publicznego, a także wykonywania tymczasowego aresztowania, kar, kar porządkowych i środków przymusu skutkujących pozbawieniem wolności[540]. Czynem zabronionym wskazanym w ustawie jest bezprawne przetwarzanie danych. Kto przetwarza dane osobowe, o których mowa w przepisach o ochronie danych osobowych, przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, choć ich przetwarzanie nie jest dopuszczalne albo do których przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch (art. 54 ust. 1 ustawy DODO). Przez naruszenie ochrony danych osobowych rozumie się 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 (art. 4 pkt 6 ustawy DODO). Forma kwalifikowana bezprawnego przetwarzania danych dotyczy danych wrażliwych[541]. Podobnie jak w ustawie o ochronie danych osobowych sprawca podlega w takim wypadku grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat trzech (art. 54 ust. 2 ustawy DODO)[542].

Niezależnie od przestępstw stypizowanych w ustawach regulujących kwestie przetwarzania danych osobowych, odpowiedzialność karną za delikty związane z ochroną danych osobowych można również przypisać na postawie norm ogólnych Kodeksu karnego. I tak przykładowo zgodnie z art. 231 k.k. każdy funkcjonariusz publiczny może zostać pociągnięty do odpowiedzialności karnej w związku z przekroczeniem uprawnień lub niedopełnieniem obowiązków[543].

Odpowiedzialność porządkowa i dyscyplinarna (zawodowa)

Odpowiedzialność porządkową należy odróżnić od odpowiedzialności dyscyplinarnej. Niewłaściwe i prawnie nieuzasadnione jest traktowanie obu pojęć jako synonimów[544]. Odpowiedzialność zawodowa jest unormowana w tzw. pragmatykach pracowniczych i służbowych. Podlegają jej m.in. urzędnicy, nauczyciele, sędziowie, adwokaci, radcowie

[539] 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 (Dz. Urz. UE L 119 z 4.05.2016, s. 89–131).

[540] Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. 2019 r., poz. 125).

[541] Ustawa wprowadza nawet własną definicję danych wrażliwych. Niedopuszczalne jest przetwarzanie danych osobowych ujawniających pochodzenie rasowe, etniczne, poglądy polityczne, przekonania religijne, światopoglądowe, przynależność do związków zawodowych oraz przetwarzanie danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej, dotyczących zdrowia, danych dotyczących seksualności i orientacji seksualnej osoby fizycznej, zwanych dalej „danymi wrażliwymi". Zob. art. 14 ust.1 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. 2019 r., poz. 125).

[542] A. Wolska-Bagińska, *Podstawy prawne przetwarzania danych osobowych w postępowaniu karnym*, Prokuratura i Prawo 2018, nr 6, s. 50.

[543] Zob. A. Adamski, *Prawo karne komputerowe*, Warszawa 2000.

[544] Zob. Z. Góral, *Odpowiedzialność porządkowa w świetle najnowszego orzecznictwa sądowego*, Praca i Zabezpieczenie Społeczne 2002, nr 11.

prawni, lekarze, pielęgniarki i położne oraz inne zawody (głównie funkcjonujące w ramach samorządów zawodowych) podlegające ocenie w ramach wewnętrznych kodeksów etycznych, zasad korporacyjnych przez własne środowisko oraz sądy dyscyplinarne. Odpowiedzialność zawodowa to zatem odpowiedzialność za naruszenie zasad wykonywania zawodu oraz za naruszenie obowiązujących w danym zawodzie zasad etyki. Reguł w tym zakresie należy każdorazowo szukać w relewantnych, sektorowych ustawach oraz kodeksach etyki czy procedurach zachowań. Przykładowo postępowanie w przedmiocie odpowiedzialności zawodowej lekarzy opiera się na przepisach ustawy z dnia 2 grudnia 2009 roku o izbach lekarskich (art. 53–112 ustawy)[545] i przepisach wykonawczych wydanych na jej podstawie w zw. z ustawa z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty[546] oraz Kodeksie etyki lekarskiej. Normy przewidują – bez uszczerbku dla odpowiedzialności karnej i cywilnej – stosowne kary dla lekarzy wykonujących zawód niezgodnie ze wskazaniami aktualnej wiedzy medycznej, dostępnymi metodami i środkami zapobiegania, rozpoznawania i leczenia chorób oraz niezgodnie z zasadami etyki zawodowej. Sąd lekarski może orzec wobec lekarza takie kary jak: (1) upomnienie, (2) nagana, (3) kara pieniężna, (4) zakaz pełnienia funkcji kierowniczych w jednostkach organizacyjnych ochrony zdrowia na okres od roku do pięciu lat, (5) ograniczenie zakresu czynności w wykonywaniu zawodu lekarza na okres od sześciu miesięcy do dwóch lat, (6) zawieszenie prawa wykonywania zawodu na okres od roku do pięciu lat, (7) pozbawienie prawa wykonywania zawodu.

Jako przykład można wskazać ustawę z dnia 26 maja 1982 r. Prawo o adwokaturze[547] regulującą odpowiedzialność adwokatów. Akt przewiduje, że adwokaci i aplikanci adwokaccy podlegają odpowiedzialności dyscyplinarnej za postępowanie sprzeczne z prawem, zasadami etyki lub godnością zawodu bądź za naruszenie swych obowiązków zawodowych, a sami adwokaci również za niespełnienie obowiązku zawarcia umowy ubezpieczenia od odpowiedzialności cywilnej. Sąd dyscyplinarny może orzec następujące kary: (1) upomnienie, (2) nagana, (3) kara pieniężna, (4) zawieszenie w czynnościach zawodowych na czas od trzech miesięcy do pięciu lat, (5) wydalenie z adwokatury[548].

Tymczasem system odpowiedzialności porządkowej jest zbudowany odrębnie. Kodeks pracy nie posługuje się pojęciem odpowiedzialności dyscyplinarnej, przewidując odpowiedzialność porządkową pracowników, która co do zasady ma jednakże inny cel niż nadzór

[545] t.j. Dz. U. z 2019 r. poz. 965, z 2020 r. poz. 1291, 2112, 2401.
[546] t.j. Dz. U. z 2021 r. poz. 790.
[547] t.j. Dz. U. z 2020 r. poz. 1651, 2320.
[548] Obok kary nagany i kary pieniężnej można orzec dodatkowo zakaz wykonywania patronatu na czas od roku do pięciu lat. Obok kary zawieszenia w czynnościach zawodowych orzeka się dodatkowo zakaz wykonywania patronatu na czas od lat dwóch do lat dziesięciu. Obok kary dyscyplinarnej można orzec dodatkowo obowiązek przeproszenia pokrzywdzonego. Orzekając ten obowiązek, sąd dyscyplinarny określa sposób jego wykonania, odpowiedni ze względu na okoliczności sprawy. Kara nagany oraz kara pieniężna pociąga za sobą utratę biernego prawa wyborczego do organu samorządu adwokackiego na czas trzech lat od dnia uprawomocnienia się orzeczenia. Kara zawieszenia w czynnościach zawodowych pociąga za sobą utratę biernego i czynnego prawa wyborczego do organu samorządu adwokackiego na czas sześciu lat od dnia uprawomocnienia się orzeczenia. Sąd dyscyplinarny może orzec podanie treści orzeczenia do publicznej wiadomości w określony sposób, jeżeli uzna to za celowe ze względu na okoliczności sprawy, o ile nie narusza to interesu pokrzywdzonego. Karę pieniężną wymierza się w granicach od półtorakrotności do dwunastokrotności minimalnego wynagrodzenia za pracę obowiązującego w dacie popełnienia przewinienia dyscyplinarnego. Wpływy z kar pieniężnych okręgowa rada adwokacka przekazuje na cele adwokatury. Kara wydalenia z adwokatury pociąga za sobą skreślenie z listy adwokatów bez prawa ubiegania się o ponowny wpis na listę adwokatów przez okres 10 lat od dnia uprawomocnienia się orzeczenia kary wydalenia z adwokatury.

na prawidłowością wykonywania zawodu czy świadczenia pracy[549]. Możliwość użycia sankcji dyscyplinarnych nie zawsze wyłącza stosowanie kar porządkowych. Niekiedy przepis stanowi, że pracownicy ponoszą odpowiedzialność porządkową lub dyscyplinarną[550], przy czym co do zasady, odpowiedzialności porządkowej nie podlegają pracownicy mianowani.

Artykuł 108 ustawy Kodeks Pracy przewiduje karę upomnienia i nagany za nieprzestrzeganie przez pracownika ustalonej organizacji i porządku w procesie pracy, przepisów bezpieczeństwa i higieny pracy, przepisów przeciwpożarowych, a także przyjętego sposobu potwierdzania przybycia i obecności w pracy oraz usprawiedliwiania nieobecności w pracy, a także karę pieniężną za nieprzestrzeganie przez pracownika przepisów bezpieczeństwa i higieny pracy lub przepisów przeciwpożarowych, opuszczenie pracy bez usprawiedliwienia, stawienie się do pracy w stanie nietrzeźwości lub spożywanie alkoholu w czasie pracy[551]. Kara pieniężna za jedno przekroczenie, jak i za każdy dzień nieusprawiedliwionej nieobecności, nie może być wyższa od jednodniowego wynagrodzenia pracownika, a łącznie kary pieniężne nie mogą przewyższać dziesiątej części wynagrodzenia przypadającego pracownikowi do wypłaty. Kary pieniężne mogą być potrącane przez pracodawcę z wynagrodzenia pracownika bez jego zgody. Wpływy z kar pieniężnych przeznacza się na poprawę warunków bezpieczeństwa i higieny pracy[552].

Skorzystanie z kar porządkowych nie wyklucza stosowania innej odpowiedzialności pracownika, nawet za to samo przewinienie (majątkowej, karnej lub zawodowej). Wymierzenie pracownikowi kary porządkowej nie wyłącza możliwości potraktowania tego samego nagannego zachowania pracownika, które było podstawą zastosowania kary, za przyczynę uzasadniającą wypowiedzenie umowy o pracę[553]. Co więcej judykatura stoi na stanowisku, że wcześniejsze wymierzenie pracownikowi kary porządkowej nie wyłącza także prawa uznania przez pracodawcę, że zachowanie to stanowi jednocześnie podstawę uzasadniającą natychmiastowe rozwiązanie umowy o pracę bez wypowiedzenia z winy pracownika. Pracodawca nie narusza

[549] Częstym błędem jest stosowanie kar porządkowych w przypadkach niewskazanych w rozdziale VI, np. w razie innych niż porządkowe uchybień przy wykonywaniu pracy, zbyt niskiej wydajności lub niewywiązywania się przez pracownika z zadań wyznaczonych przez przełożonego. Niektórzy pracodawcy stosują kary porządkowe nie tyle w razie naruszenia przez pracownika przepisów dotyczących organizacji i porządku pracy, ile raczej sposobu świadczenia pracy. Jednak odpowiedzialność porządkowa nie może zastępować takich instytucji, jak np. wypowiedzenie zmieniające. Zgodnie ze stanowiskiem SN, w świetle obowiązujących przepisów prawa pracy wypowiedzenie warunków płacy wprawdzie nie jest karą porządkową, ale może być środkiem dyscyplinującym. Zob. wyrok SN z 26.7.1979 r., I PR 64/79, OSNC 1980, Nr 1, poz. 17. Por. Z. Góral, *Odpowiedzialność porządkowa w świetle najnowszego orzecznictwa sądowego*, Praca i Zabezpieczenie Społeczne 2002, nr 11.

[550] Por. art. 34 ustawy z 16 września 1982 r. o pracownikach urzędów państwowych (t.j. Dz. U. z 2021 r. poz. 2447, 2448) oraz art. 75 ustawy z 26 stycznia 1982 r. Karta nauczyciela (t.j. Dz. U. z 2021 r. poz. 1762).

[551] Szerzej zob. *Kodeks pracy. Komentarz*, red. A. Sobczyk, Warszawa 2017.

[552] Kara nie może być zastosowana po upływie 2 tygodni od powzięcia wiadomości o naruszeniu obowiązku pracowniczego i po upływie 3 miesięcy od dopuszczenia się tego naruszenia. Kara może być zastosowana tylko po uprzednim wysłuchaniu pracownika. Jeżeli z powodu nieobecności w zakładzie pracy pracownik nie może być wysłuchany, bieg dwutygodniowego terminu przewidzianego w § 1 nie rozpoczyna się, a rozpoczęty ulega zawieszeniu do dnia stawienia się pracownika do pracy. O zastosowanej karze pracodawca zawiadamia pracownika na piśmie, wskazując rodzaj naruszenia obowiązków pracowniczych i datę dopuszczenia się przez pracownika tego naruszenia oraz informując go o prawie zgłoszenia sprzeciwu i terminie jego wniesienia. Odpis zawiadomienia składa się do akt osobowych pracownika. Przy stosowaniu kary bierze się pod uwagę w szczególności rodzaj naruszenia obowiązków pracowniczych, stopień winy pracownika i jego dotychczasowy stosunek do pracy. Jeżeli zastosowanie kary nastąpiło z naruszeniem przepisów prawa, pracownik może w ciągu 7 dni od dnia zawiadomienia go o ukaraniu wnieść sprzeciw. O uwzględnieniu lub odrzuceniu sprzeciwu decyduje pracodawca po rozpatrzeniu stanowiska reprezentującej pracownika zakładowej organizacji związkowej. Nieodrzucenie sprzeciwu w ciągu 14 dni od dnia jego wniesienia jest równoznaczne z uwzględnieniem sprzeciwu. Pracownik, który wniósł sprzeciw, może w ciągu 14 dni od dnia zawiadomienia o odrzuceniu tego sprzeciwu wystąpić do sądu pracy o uchylenie zastosowanej wobec niego kary. W razie uwzględnienia sprzeciwu wobec zastosowanej kary pieniężnej lub uchylenia tej kary przez sąd pracy, pracodawca jest obowiązany zwrócić pracownikowi równowartość kwoty tej kary. Karę uważa się za niebyłą, a odpis zawiadomienia o ukaraniu usuwa z akt osobowych pracownika po roku nienagannej pracy. odpowiednio w razie uwzględnienia sprzeciwu przez pracodawcę albo wydania przez sąd pracy orzeczenia o uchyleniu kary. Pracodawca może, z własnej inicjatywy lub na wniosek reprezentującej pracownika zakładowej organizacji związkowej, uznać karę za niebyłą przed upływem tego terminu. Zob. art. 109–112 ustawy Kodeks pracy (t.j. Dz. U. z 2021 r., poz. 1162).

[553] Zob. wyrok Sądu Najwyższego z dnia 25 października 1995 roku, I PRN 77/95.

dóbr osobistych pracownika nawet wówczas, gdy kara porządkowa w postępowaniu sądowym zostanie uznana za niesłusznie zastosowaną. Stanowisko to także znajduje potwierdzenie w orzecznictwie. W ocenie Sądu Najwyższego stosowanie kar porządkowych nie może stanowić dyskryminacji pracownika, tym bardziej w sytuacji, w której prawidłowość nałożenia kar została zweryfikowana w toczącym się wskutek odwołania od tych kar postępowaniu[554]. Pracodawcy nie wolno natomiast zmieniać procedury karania na niekorzyść pracownika ani tym bardziej stosować innych kar niż wymienione (gdyby takie postanowienia znalazły się w szczególnych źródłach prawa pracy, należałoby je uznać za nieobowiązujące).

Możliwość wyegzekwowania odpowiedzialności porządkowej i dyscyplinarnej, za naruszenie zasad przetwarzania danych osobowych, pod rządami aktu prawnego z 1997 roku, przewidywał wprost art. 17 ustawy. Zgodnie z tym przepisem uprawnionym do żądania wszczęcia postępowania dyscyplinarnego był kontrolujący inspektor – pracownik GIODO, w oparciu o wyniki przeprowadzonej kontroli. Żądanie powinno było zostać skierowane do podmiotu, który dysponuje uprawnieniem do wszczęcia i prowadzenia właściwego postępowania przeciwko osobie winnej dopuszczenia uchybień w zakresie administrowania danymi osobowymi. Podmiot ten nie był w żaden sposób związany żądaniem wszczęcia postępowania dyscyplinarnego, jak również nie był związany ocenami dokonanymi przez inspektora w zakresie jego uwag, co do przypisania określonym osobom odpowiedzialności z tytułu stwierdzonych uchybień w procesie przetwarzania danych osobowych. Wszczęcie zatem procedury dyscyplinarnej czy porządkowej uzależnione było od arbitralnej decyzji dysponenta takiego postępowania. Inspektor jednak mógł żądać poinformowania go o wynikach postępowania lub podjętych przez podmiot krokach, w sprawie skierowanego do niego żądania. Powyższe kompetencje obejmowałyby zarówno żądanie wszczęcia postępowania porządkowego, jak i dyscyplinarnego.

Zbieżne z art. 17 ustawy z 1997 roku uprawnienie odnaleźć można również w porządku prawnym po wejściu w życie RODO oraz ustawy ochronie danych osobowych z 2018 roku. Art. 58 ustawy przewiduje, że jeżeli Prezes Urzędu, na podstawie posiadanych informacji uzna, że doszło do naruszenia przepisów dotyczących przetwarzania danych osobowych, może żądać wszczęcia postępowania dyscyplinarnego lub innego przewidzianego prawem postępowania przeciwko osobom, które dopuściły się naruszeń, i poinformowania go, w określonym terminie, o wynikach tego postępowania i podjętych działaniach. Stanowisko to powielenie rozwiązania prawnego z 1997 roku ze wszystkimi, wyżej opisanymi, konsekwencjami prawnymi. Zmiana polega na tym, że w obecnym stanie prawnym relewantne uprawnienie przysługuje Prezesowi Urzędu i nie jest tak ściśle powiązane z kontrolą, o czym świadczy umiejscowienie tegoż przepisu. Poprzednio żądanie wszczęcia postępowania było możliwe jedynie w sytuacji, gdy inspektor stwierdzał naruszenie przepisów w wyniku kontroli.

[554] Zob. wyrok Sądu Najwyższego z dn. 18 lutego 2015 roku, I PK 171/14. Por. wyrok Sądu Najwyższego z dnia 10 grudnia 2012 roku, I PK 147/12).

Uprawnienie do skorzystania z tego środka przysługiwało kontrolującemu inspektorowi[555]. Aktualnie Prezes Urzędu może skorzystać z tego prawa niezależnie od samego postępowania kontrolnego. Nadto komentatorzy wskazują na obligatoryjność wszczęcia odpowiedniego postępowania. Za takim stanowiskiem, przemawia choćby nałożenie obowiązku poinformowania o wynikach postępowania[556].

Adresatem żądania może być nie tylko kontrolowany przez organ nadzorczy administrator lub podmiot przetwarzający, ale każdy podmiot uprawniony na mocy przepisów do wszczęcia i przeprowadzenia właściwego postępowania wobec osoby, która dopuściła się naruszeń. Stwierdzenie przez Prezesa Urzędu, że doszło do naruszenia przepisów o ochronie danych (przepisów dotyczących przetwarzania danych), uprawnia organ nadzorczy do podjęcia, wobec administratora lub podmiotu przetwarzającego, określonych przepisami środków (o których mowa w art. 58 rozporządzenia), w tym nałożenia administracyjnej kary pieniężnej. Prezes Urzędu jest również uprawniony do tego, aby zwrócić się do administratora lub podmiotu przetwarzającego z żądaniem wszczęcia postępowania dyscyplinarnego lub innego przewidzianego prawem postępowania przeciwko osobom, które dopuściły się naruszeń. W świetle przepisów ustawy (zarówno poprzedniej, jak i obecnej) naruszenie obowiązków pracowniczych związanych z ochroną danych osobowych może być – w zależności od podstawy nawiązania stosunku pracy – przedmiotem odpowiedzialności dyscyplinarnej lub porządkowej (w przypadku pracowników mianowanych) albo tylko porządkowej (np. w przypadku pracowników zatrudnionych na podstawie umów o pracę). Ustalenia te pozostają nadal aktualne[557].

Podsumowanie

Przepisy rozporządzenia, sektorowe oraz ogólne przewidują szereg różnych form odpowiedzialności za delikty przełamujące porządek prawny GDPR. O ile odpowiedzialność porządkowa (pracownicza), dyscyplinarna (korporacyjna), oraz przede wszystkim cywilna, wynikająca z prawa powszechnego pozostały bez zmian, w stosunku do reformy systemu wynikającej z RODO, to począwszy od 25 maja 2018 roku radykalnej przebudowie uległ system odpowiedzialności administracyjnej, karnej oraz cywilnej *lex specialis*.

I tak począwszy od końca ogólne podstawy wynikające z prawa cywilnego uległy poszerzeniu o możliwość bezpośredniego powołania się na przepisy unijne dotyczące odpowiedzialności odszkodowawczej za naruszenie zasad ochrony danych osobowych. Przyznano bowiem każdej osobie fizycznej, której dobra zostały naruszone, prawo do wystąpienia z odrębnym roszczeniem o zapłatę odszkodowania za naruszenie przepisów ochrony danych osobowych.

[555] Zob. *Ustawa o ochronie danych osobowych. Komentarz*, red. B. Marcinkowski, Warszawa 2018.
[556] Tak Natalia Zawadzka w komentarzu do rozporządzenia pod redakcją Dominika Lubasza. Zob. N. Zawadzka, *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, red. D. Lubasz, E. Bielak-Jomaa, Warszawa 2017.
[557] P. Fajgielski, *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2018.

Wprowadzono zatem nową, samodzielną podstawę dochodzenia roszczeń cywilnoprawnych w postaci art. 82 RODO. Adresatem powództwa za poniesioną szkodę może być administrator lub podmiot przetwarzający (procesor). Postępowanie w sprawie zasądzenia roszczeń odszkodowawczych, dochodzonych na podstawie art. 82 ust. 1 rozporządzenia za poniesioną przez osobę fizyczną szkodę majątkową lub niemajątkową, toczy się w oparciu o przepisy Kodeksu postępowania cywilnego, z uwzględnieniem szczególnych regulacji przewidzianych w ustawie o ochronie danych osobowych w rozdziale 10. Sądem właściwym do rozpoznania tego typu spraw – niezależnie od wartości przedmiotu sporu – jest sąd okręgowy. Ustawa nie przewiduje żadnych szczególnych regulacji dotyczących właściwości miejscowej sądu, a zatem należy uznać, że będzie to sąd właściwości ogólnej pozwanego. Oczywiście wystąpienie z roszczeniem odszkodowawczym nie wyłącza możliwości dochodzenia innych roszczeń z tytułu naruszenia przepisów o ochronie danych osobowych na zasadach ogólnych.

W przypadku systemu odpowiedzialności karnej panującego w Polsce do 2018 roku panowało powszechne przekonanie, że był obarczony wieloma dysfunkcjonalnościami. System przepisów karnych zawartych w rozdziale 8 ustawy o ochronie danych osobowych był nie tylko mało efektywny, ale iluzoryczny z uwagi na konstrukcję przestępstw stypizowanych w art. 53 i 54 ustawy, jako typów wyłącznie umyślnych, czy też z ograniczenia stosowania art. 49 ust. 1 i 2 ustawy do działania na zbiorze danych osobowych. Jednocześnie wskazywano na opresyjność i tym samym zbędność norm karnych penalizujących takie zachowania, jak niezgłoszenie zbioru danych osobowych do rejestracji czy naruszenie obowiązków informacyjnych względem osób, których dane dotyczą. Część norm karnych przez wiele lat funkcjonowania w obrocie prawnym była *de facto* martwa. Porównując rozwiązania zaproponowane w aktualnie obowiązującej ustawie o ochronie danych osobowych, z konstrukcją odpowiedzialności karnej obowiązującą do 2018 roku, warto zauważyć, że nastąpiła redukcja – pod względem ilościowym – typów przestępstw. Jeszcze na etapie uzasadnienia do projektu ustawy normodawca wskazywał, iż odpowiedzialność karna powinna odnosić się do najpoważniejszych naruszeń przepisów, stanowiąc jedynie uzupełnienie dla odpowiedzialności administracyjnej oraz cywilnej – co znalazło wyraz w nowej ustawie (zmniejszono ilość norm karnych z sześciu do dwóch).

Największą rewolucję przeszedł jednak system odpowiedzialności administracyjnej. Podobnie jak w przypadku sankcji karnych temu modelowi odpowiedzialności zarzucano iluzoryczność. Sankcje administracyjne były nieproporcjonalnie niskie w porównaniu do potencjalnych rozmiarów szkód. Często występującym problemem było zjawisko tzw. „forum shoppingu" (wybierania organu nadzoru pod kątem względności sankcji). Oczywistym skutkiem reformy systemu odpowiedzialności administracyjnej stała się nie tylko wysokość potencjalnych sankcji (podniesionych w sposób rewolucyjny), ale przede wszystkim efektywność nakładanych kar. I tak, o ile stare przepisy mierzyły się z zarzutem pozorności nakładanych kar (w szczególności wobec gigantów teleinformatycznych) oraz zjawiskiem wybierania

sobie organów nadzoru oraz systemu kar poszczególnych państwa członkowskich, to nowy model GDPR urealnił system kar za naruszenia standardów ODO. Przykłady prowadzonych postępowań potwierdzają tę tezę.

W styczniu 2019 roku koncern Google został obciążony karą 57 milionów euro, w lipcu 2021 roku amerykański koncern Amazon poinformował, że ma zapłacić 887 mln dol. (746 mln euro) za naruszenie unijnych zasad ochrony danych. Najgłośniejsza była ugoda związana z aferą Cambridge Analytica. W Polsce pierwsza kara została nałożona w marcu 2019 roku. Łącznie, w tym roku w toku przeprowadzonych postępowań, w ośmiu przypadkach Prezes Urzędu Ochrony Danych Osobowych, stosując przysługujące mu rozwiązania naprawcze przewidziane w art. 58 ust. 2 RODO, zdecydował o nałożeniu kary administracyjnej. Wysokość nałożonych kar kształtowała się następująco: (1) 55 750,50 zł. na Dolnośląski Związek Piłki Nożnej z siedzibą we Wrocławiu, (2) 2 830 410 zł. na Morele.Net Sp. z o.o. z siedzibą w Krakowie, (3) ponad 943 tys. zł na Bisnode Polska Sp. z o.o., (4) ponad 201 tys. zł na ClickQuickNow Sp. z o.o., (5) 40 tys. zł. na burmistrza miasta Aleksandrów Kujawski za niezawieranie umów powierzenia, (6) 2 tys. zł. na wspólnotę mieszkaniową, (7) 8 tys. zł. na spółkę zarządzającą nieruchomościami oraz (8) 30 tys. na spółkę zajmującą się ochroną osób i mienia. W 2020 roku Prezes UODO wszczął z urzędu 23 postępowania w sprawie nałożenia kary za brak współpracy z organem nadzorczym poprzez nieudzielenie mu informacji niezbędnych do realizacji jego zadań. Decyzjami nakładającymi administracyjne kary 153 pieniężne w 2020 r. zakończyły się 3 z nich, z czego 2 decyzje stały się prawomocne z uwagi na niewniesienie skarg do Wojewódzkiego Sądu Administracyjnego, zaś pozostała 1 decyzja na skutek wniesionej skargi podlega kontroli sądowej – jednak w roku 2020 nie zapadło prawomocne orzeczenie sądu w jej przedmiocie. Jedno postępowanie zakończyło się na początku 2021 roku nałożeniem kary w kwocie ponad 85 588 zł (20 000 EUR).

Na początku 2022 roku polski Urząd Ochrony Danych Osobowych nałożył najwyższą w swej historii karę za naruszenie RODO. Około 4,9 mln zł. ma zapłacić dostawca prądu i gazu, spółka Fortum Marketing and Sales Polska, za to, że nie zadbał wystarczająco o dane swych klientów[558]. Jeszcze pod koniec 2021 roku Urząd Ochrony Danych Osobowych nałożył na Santander Bank Polska karę administracyjną w wysokości ponad 545 tys. zł m.in. za naruszenia poufności danych[559].

Polska zajmuje 13. miejsce pod względem łącznej wysokości kar nałożonych od chwili wejścia w życie przepisów RODO w 2018 roku. W regionie Europy Środkowo-Wschodniej

[558] Kara to wynik braku nadzoru nad firmą, która na zlecenie administratora danych wdrażała nowe narzędzie informatyczne. Podmiot przetwarzający pracował na niezabezpieczonych danych, kopiując bazę klientów na niezabezpieczony serwer. Bezpośrednią winę za incydent ponosi więc podwykonawca, który również został ukarany i ma zapłacić 250 tys. zł. Dużo wyższa sankcja nałożona na Fortum wynika z faktu, że to ta spółka jako administrator danych powinna wdrożyć procedury gwarantujące bezpieczeństwo danych. Zob. S. Wikariak, *Rekordowa kara za naruszenie RODO*, https://www.gazetaprawna.pl/firma-i-prawo/artykuly/8369936,naruszenie-rodo-kary-fortum-marketing-and-sales-polska.html, [dostęp: 15.02.2022]. Por. M. Rzemek, *4,9 mln zł – nowy rekord kary za naruszenie RODO*, https://www.rp.pl/dane-osobowe/art35775391–4-9-mln-zl-nowy-rekord-kary-za-naruszenie-rodo, [dostęp: 15.02.2022].

[559] Były pracownik banku posiadał nieuprawniony dostęp do profilu płatnika na Platformie Usług Elektronicznych ZUS (PUE ZUS). W wyniku tego mógł on przeglądać znajdujące się na profilu płatnika Santander Bank Polska dane osób zatrudnionych w banku. Urząd uznał, że doszło do naruszenia poufności danych, które wiąże się jednocześnie z zaistnieniem wysokiego ryzyka dla naruszenia praw lub wolności osób, których dane dotyczą. Zdaniem organu nadzorczego osoby te należało zawiadomić o zaistniałym incydencie. Zob. *Ponad pół miliona złotych kary dla Santander Bank Polska. Były pracownik mógł przeglądać dane*, https://businessinsider.com.pl/finanse/ponad-pol-miliona-zlotych-kary-dla-santander-bank-polska-byly-pracownik-mogl/0x4pqmh, [dostęp: 15.02.2022].

wyższe łączne kary nałożył jedynie regulator w Bułgarii i wyniosły 3,2 mln euro. Kwoty te i tak pozostają skromne w relacji do wysokości kar nałożonych przez europejskie organy regulacyjne na zachód od Odry. Jak wynika z raportu międzynarodowej kancelarii prawnej DLA Piper, rekordowa kara w kwocie 746 mln euro została nałożona w 2021 roku w Luksemburgu, kolejna przez organ regulacyjny w Irlandii w kwocie 225 mln euro. Trzecia najwyższa w historii kara za naruszenie przepisów RODO została nałożona we Francji i wyniosła 50 mln euro. Organy nałożyły w 2021 roku niemal 1,1 mld euro kar z tytułu naruszeń RODO, co oznacza siedmiokrotny wzrost w porównaniu z rokiem wcześniejszym[560]. Na początku 2022 roku regulator z siedzibą w Luksemburgu już wszczął postępowanie przeciwko spółce Amazon Europe Core SARL. W grę wchodzi kara w wysokości aż 425 000 000 dolarów (ponad 1,5 miliarda złotych). W przypadku jej nałożenia, spółka stałaby się nowym niechlubnym rekordzistą pod względem wysokości jednostkowej kary nałożonej przez unijne organy nadzorcze[561].

Analiza przypadków oraz dotychczasowej administracyjnej linii orzeczniczej wskazuje, że skala działania opisanych podmiotów uzasadniała wysokie kary, co z kolei motywuje twierdzenie, że nowe przepisy wreszcie wyposażyły organy nadzorcze w realne narzędzia stosowania prawa. Należy także pamiętać, że zdecydowana większość decyzji Prezesa UODO była skarżona do Wojewódzkiego Sądu Administracyjnego w Warszawie. To implikuje przekonanie, iż w niedalekiej przyszłości ukształtuje się stosowna, sądowa linia orzeczniczej w sprawach rozpatrywanych z zakresu ochrony danych osobowych.

Pomimo wprowadzenia narzędzi pozwalających stosować wysokie sankcje administracyjne ujawnił się w Polsce znaczący problem z ich egzekucją. Przez cztery lata obowiązywania RODO polski Urząd Ochrony Danych Osobowych – według danych międzynarodowej kancelarii prawnej DLA Piper – polski regulator nałożył 40 kar administracyjnych na kwotę 2,2 mln euro, z czego udało się ściągnąć łączną kwotę 150 tys. zł. tylko od czterech podmiotów. Tak wygląda w Polsce w praktyce egzekwowanie unijnego prawa dotyczącego ochrony danych osobowych[562].

[560] K. Sobczak, *Siedmiokrotny wzrost kar za naruszenie RODO w Europie*, https://www.prawo.pl/prawo/kary-za-naruszenie-rodo-w-europie-duzy-wzrost,512924.html, [dostęp: 15.02.2022].

[561] Postępowanie prowadzone jest przez organ nadzorczy z Luksemburga, nie mniej uział w nim wezmą również pozostałe unijne organy nadzorcze. Regulator sięgnął bowiem do mechanizmu współpracy (art. 60 RODO – tzw. mechanizm *„one-stop shop"*), co wynika z faktu, że potencjalne naruszenia giganta obejmują swoim zakresem osoby fizyczne również z innych krajów UE. W związku z zastosowaniem mechanizmu współpracy, ostateczna treść decyzji CNPD w tej sprawie (również co do wysokości nałożonej kary) zostanie ustalona wspólnie z pozostałymi unijnymi organami nadzorczymi. *Kara rekordowej wysokości za naruszenie przepisów RODO?*, https://gdpr.pl/kara-rekordowej-wysokosci-za-naruszenie-przepisow-rodo, [dostęp: 15.02.2022].

[562] M. Krawiel, S. Jadczak, *Miały być gigantyczne kary. Jest kapiszon. RODO po polsku*, https://www.money.pl/gospodarka/miały-byc-gigantyczne-kary-jest-kapiszon-rodo-po-polsku-6736281656224544a.html, [dostęp: 15.02.2022].

Praktyczne aspekty reformy wynikającej z RODO. Poprawność formalno-prawna dokumentacji systemu ochrony danych osobowych

Etapy wdrażania systemu ochrony danych osobowych w jednostce organizacyjnej

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 weszło w życie 25 maja 2016 roku z odroczeniem stosowania od 25 maja 2018 roku. Dwuletnie *vacatio legis* pozwoliło uzyskać czas na analizę wpływu przepisów na poszczególne branże i instytucje oraz na zdefiniowanie wynikających z nich obowiązków. Implementacja nowych norm wymagała ponownego zdefiniowania charakteru obowiązków, którym podlegają administratorzy danych oraz pozostali adresaci przepisów, a następnie oceny stanu zgodności[563]. Stanowiło to podstawę do opracowania przez administratorów danych lub przez konsultantów zewnętrznych (w ramach *outsourcingu*) – planu działań dostosowawczych, w tym kolejny czynności powinny obejmować co najmniej działania jak następuje:

- sprawdzenie świadomości oraz gotowości przedsiębiorcy do wdrożenia nowych procedur bezpieczeństwa danych osobowych,
- przeprowadzenia audytu zgodności systemu bezpieczeństwa danych osobowych w jednostce organizacyjnej z aktualnymi przepisami,
- opracowanie i wdrożenie procedur pozwalających na stwierdzenie zgodności z systemu z aktualnie obowiązującymi przepisami,
- opracowanie raportu w zakresie przygotowania i gotowości jednostki organizacyjnej do wdrożenia i przyjęcia nowych procedur wynikających z rozporządzenia,
- opracowanie i wdrożenie w jednostce organizacyjnej wszystkich procedur pozwalających na stwierdzenie zgodności z systemu z przepisami rozporządzenia[564].

Potrzebny w tym zakresie był czas do analizy wpływu przepisów na poszczególne sfery i instytucje w danej jednostce organizacyjnej – pod kątem jej specyfiki branżowej i funkcjonalnej – oraz na zdefiniowanie wynikających z niego obowiązków. Implementacja norm wymagała zdefiniowania nowych obowiązków, a następnie oceny obecnego stanu zgodności

[563] Zob. *Przygotowanie organizacji do stosowania RODO. Ochrona danych w okresie przejściowym i po wejściu przepisów w życie,* red. M. Korga, wyd. PRESSCOM, Wrocław 2017. Por. T. Banyś, J. Łuczak, *Ochrona danych osobowych w praktyce. Jak uniknąć błędów i ich konsekwencji prawnych*, wyd. PRESSCOM, Wrocław 2017.

[564] Szerzej zob. M. Krzysztofek, *Sprawdzenie gotowości instytucji do wdrożenia reformy ochrony danych osobowych*, Informacja w administracji publicznej 2017, nr 4.

z tymi obowiązkami, wreszcie dopasowanie modelu organizacyjnego, logistycznego i technicznego administratora do nowych wymogów. Powyższe opracowania administrator winien zrealizować własnymi aktywami, względnie poprzez *outsourcing* usługi w ramach zewnętrznych konsultacji w oparciu o doświadczenie specjalistów przy udziale funkcjonującego w danej jednostce organizacyjnej Inspektora Ochrony Danych. W tym zakresie procedury co najmniej powinny obejmować przestrzenia jak następuje[565].

- audyt i ewaluacja aktualnego systemu bezpieczeństwa danych osobowych,
- posiadanie prawidłowej dokumentacji, w tym: (a) Polityki Ochrony Danych Osobowych, (b) Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych oraz nowych dokumentów wymaganych prawem, w szczególności Rejestru Czynności Przetwarzania Danych, Analizy Ryzyka Przetwarzania Danych Osobowych (*risk based approach*) w fazie projektowania (*privacy by design*), oraz w fazie przetwarzania danych osobowych (*privacy by default*), Oceny Skutków Przetwarzania Danych Osobowych (*privacy impact assessment*),
- powołanie Inspektora Ochrony Danych, oraz zapewnienie mu odpowiednich zasobów i gwarancji niezależności – przy rozważeniu możliwości/konieczności powołania IOD dla danej grupy kapitałowej, czy rodziny przedsiębiorstw – co wynika z nowej możliwości przetwarzania wspólnie danych osobowych przez grupy kapitałowe,
- stosowanie mechanizmów *privacy by design* i *privacy by default*, w tym dokonanie przedsięwzięć oceny ryzyka przetwarzania danych osobowych w firmie oraz wstępnej (w fazie projektowania) i docelowej (w fazie stosowania) oceny skutków przetwarzania,
- dostosowanie fizyczne, techniczne, organizacyjne, logistyczne i społeczne firmy do wymogów bezpieczeństwa – w szczególności wprowadzenia środków bezpieczeństwa, o których mowa w art. 32 rozporządzenia,
- wprowadzenie środków pozwalających (technicznie, funkcjonalnie oraz prawnie) na przestrzeganie podstawowych zasad przetwarzania, w tym warunków uzyskania zgody oraz praw osób, których dane dotyczą, w tym m.in.: prawa dostępu do danych, prawa do sprostowania, prawa do bycia zapomnianym, prawa do ograniczenia przetwarzania, prawa do przenoszenia danych, prawa do wniesienia sprzeciwu, prawa do tego, by nie podlegać decyzji, która opera się wyłącznie na zautomatyzowanym przetwarzaniu w tym profilowaniu, jak również zasad transferu danych osobowych do państw trzecich lub organizacji międzynarodowych oraz wszelkich obowiązków wynikających z prawa państwa członkowskiego przyjętego w związku z zapewnieniem wolności wypowiedzi i informacji, przetwarzaniem danych w kontekście zatrudnienia, przetwarzaniem danych w celach archiwalnych, naukowych, historycznych, statystycznych, przetwarzaniem danych przez kościoły i związki wyznaniowe,

[565] Szerzej zob. *Tworzenie systemu ochrony danych osobowych krok po* kroku, red. I. Kuc, wyd. Difin S.A., Warszawa 2016.

- wprowadzenie środków pozwalających (technicznie, funkcjonalnie oraz prawnie) na dokonywanie rejestru czynności przetwarzania danych osobowych, zgodnie z wytycznymi, o których mowa w art. 30 rozporządzenia.
- wprowadzenie środków pozwalających (technicznie, funkcjonalnie oraz prawnie) na wprowadzenie kontroli nad profilowaniem,
- wprowadzenie środków pozwalających (technicznie, funkcjonalnie oraz prawnie) na dokonywanie pseudonimizacji przetwarzanych danych osobowych,
- wprowadzenie środków pozwalających (technicznie, funkcjonalnie oraz prawnie) na weryfikację zgody od opiekuna dziecka poniżej 16. roku życia w przypadku oferowania dziecku usług społeczeństwa informacyjnego,
- odpowiednie uregulowanie relacji pomiędzy współadministratorami zgodnie z wytycznymi określonymi w art. 26 rozporządzenia oraz z podmiotem przetwarzającym zgodnie z wytycznymi określonymi w art. 28 rozporządzenia.
- dopełnienia obowiązku wyznaczenia przedstawiciela na terenie Unii,
- dopełnienie obowiązku wyraźnego wskazania osób upoważnionych przez administratora danych do przetwarzania danych osobowych w firmie,
- wprowadzenie środków pozwalających (technicznie, funkcjonalnie oraz prawnie) na skuteczne realizowanie obowiązku współpracy z organem nadzorczym, zgodnie z wytycznymi określonymi w art. 31 rozporządzenia, w tym pozwalających na terminowego i zgodne z prawem zgłoszenia naruszenia ochrony danych osobowych organowi nadzorczemu, czy obowiązek uprzednich konsultacji z organem nadzorczym, w przypadku gdyby dany rodzaj przetwarzania powodował wysokie ryzyko, co potwierdziła ocena skutków dla ochrony danych,
- wprowadzenie środków pozwalających (technicznie, funkcjonalnie oraz prawnie) na skuteczne realizowanie obowiązku zawiadomienia osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, zgodnie z wytycznymi z art. 34 rozporządzenia,
- wdrożenie kompleksowego – nowego systemu bezpieczeństwa danych osobowych,
- przeprowadzenie szkoleń dla pracowników przetwarzających dane osobowe.

Świadomość administratorów a wdrożenia nowych procedur ochrony danych osobowych

Sprawdzenie gotowości jednostki organizacyjnej do wdrożenia reformy ochrony danych osobowych wymagało przeprowadzenia audytów ochrony danych, które winny uwzględniać badanie świadomości kadry zarządczej (na stanowiskach wszystkich szczebli) oraz pozostałych uczestników (np. pracowników) wewnętrznej struktury w zakresie nowych przepisów oraz konsekwencji z nich wynikających. Opracowywanie planów audytów jest początkiem procesu badania zgodności wewnętrznego systemu ODO z wymogami norm prawnych. Przy czym należy mieć świadomość, iż każda osoba zaangażowana (bez względu na formę zatrudnienia[566])

[566] Należy mieć na uwadze, że ochrony danych osobowych powinna zostać uruchomiona już na etapie rekrutacji. Szerzej zob. (1) G. Sibiga, *Przetwarzanie*

w proces przetwarzania danych osobowych u administratora danych musi przestrzegać procedur bezpieczeństwa danych osobowych[567].

Po pierwsze, należało dokonać pełnej aktualizacji dokumentacji wewnętrznego systemu ochrony danych osobowych, w tym w szczególności – zgodnie z art. 24 rozporządzenia – opracować i wdrożyć nową Politykę Ochrony Danych Osobowych[568].

Po drugie administratorzy danych musieli ocenić, czy nie objął ich obowiązek powołania Inspektora Ochrony Danych (IOD), nawet jak wcześniej zrezygnowali z powołania Administratora Bezpieczeństwa Informacji (ABI). Trzeba było ocenić, czy kandydat na IOD dawał gwarancję odpowiedniego poziomu wiedzy fachowej oraz niezależnego wykonywania obowiązków, ewentualnie rozważyć *outsourcing* tej funkcji lub jej zewnętrzne wsparcie. Warto przypomnieć, że ustawa o ochronie danych osobowych z 1997 roku wprowadziła od 1 stycznia 2015 roku fakultatywność powoływania Administratora Bezpieczeństwa Informacji. Ponadto na mocy nowej polskiej ustawy o ochronie danych Inspektor Ochrony Danych w określonych sytuacjach IOD *ex lege* zastępował ABI, pełniąc swoją funkcję do dnia 1 września 2018 r., chyba że przed tym dniem administrator danych zawiadomił Prezesa Urzędu Ochrony Danych Osobowych o wyznaczeniu innej osoby na funkcję IOD. Natomiast zgodnie z rozporządzeniem 2016/679 wyznaczenie Inspektora Ochrony Danych stało się co do zasady zalecane, natomiast obowiązkowe w wyraźnie wskazanych w RODO trzech przypadkach:

1) gdy przetwarzania dokonują organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości (przesłanka ta nie dotyczy więc zwykłych przedsiębiorców);
2) gdy główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę (dotyczy to więc przykładowo profilowania i oceny osób w ramach szacowania ryzyka, w celu przyznania zniżek składek ubezpieczeniowych)[569];
3) gdy główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych (np. danych ujawniających poglądy polityczne czy też danych dotyczących zdrowia przetwarzanych przez szpitale), oraz danych dotyczących wyroków skazujących i naruszeń prawa.

i ochrona danych osoby ubiegającej się o zatrudnienie w świetle przepisów prawa pracy, Radca Prawny 2005, nr 2, (2) G. Sibiga, *Zakres stosowania ustawy o ochronie danych osobowych do przetwarzania danych osobowych pracowników i osób ubiegających się o zatrudnienie*, Monitor Prawa Pracy 2012, nr 3.

[567] Szerzej zob. *Wdrażanie systemu ochrony danych osobowych. Praktyczny przewodnik krok po* kroku, red. I. Kuc, wyd. Difin S.A., Warszawa 2016.

[568] Zob. *Dokumentacja ochrony danych osobowych. Praktyczny przewodnik krok po kroku,* red. I. Kuc, wyd. Difin S.A., Warszawa 2016.

[569] W wytycznych Grupy Roboczej art. 29 wskazano następujące przykłady takiej działalności: (a) obsługa sieci telekomunikacyjnej lub świadczenie usług telekomunikacyjnych, (b) przekierowywanie poczty elektronicznej, (c) działania marketingowe oparte na danych, (d) profilowanie i ocenianie dla celów oceny ryzyka (na przykład dla celów oceny ryzyka kredytowego, ustanawiania składek ubezpieczeniowych, zapobiegania oszustwom, wykrywania prania pieniędzy), (e) śledzenie lokalizacji (na przykład przez aplikacje mobilne), (f) programy lojalnościowe czy reklama behawioralna, (g) monitorowanie danych dotyczących zdrowia i kondycji fizycznej za pośrednictwem urządzeń przenośnych, (h) monitoring wizyjny, (i) urządzenia skomunikowane np. inteligentne liczniki, inteligentne samochody, automatyka domowa, itp. 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.

Należy zauważyć, że nawet jeśli określony podmiot nie spełnia żadnej z wyżej powołanych przesłanek i nie jest zobowiązany do powołania Inspektora Ochrony Danych, to i tak powinien udokumentować przeprowadzenie wewnętrznej procedury, która pozwoliła mu na ustalenie, że nie należy do żadnej grupy podmiotów, które muszą powołać IOD. Stąd nawet jeżeli powołanie IOD nie stało się obligatoryjne, to z uwagi na doniosłość obowiązków administratora danych (względnie procesora), na pewno zalecane. Przy tym należy pamiętać, iż pozycja prawna Inspektora Ochrony Danych nie jest powieleniem, a tym bardziej nie pokrywa się z pozycją organizacyjną Administratora Bezpieczeństwa Informacji (funkcjonującego na starych przepisach)[570]. O ile ABI realizował obowiązki w imieniu administratora danych i był *de facto* jego pełnomocnikiem w zakresie realizacji bezpieczeństwa danych osobowych w jednostce organizacyjnej to IOD jest bardziej strażnikiem ochrony danych osobowych z perspektywy interesów nie tyle dysponentów danych, co ich właścicieli w danej jednostce organizacyjnej[571].

Po trzecie administratorzy powinni byli zweryfikować prawidłowość podstaw prawnych przetwarzania danych. Przegląd mógł ujawnić luki w praktyce działania administratora, często wynikające z tego, że posługiwania się z zautomatyzowanymi systemami informatycznymi. Audyt powinien pozwolić również wpisać się w badanie gotowości do zapewnienia zasad „prywatności od samego początku" i „prywatności jako opcji domyślnej". Wymagają one, już na etapie projektowania usług, systemów i aplikacji, zastosowania środków technicznych i organizacyjnych, takich jak pseudonimizacja, aby zapewnić m.in. minimalny zakres danych konieczny do osiągnięcia celu przetwarzania.

Po czwarte należało przyjrzeć się zasadom odbierania zgody na przetwarzanie danych. Przedmiotem badania musiało być to, czy klauzula służąca do odbierania zgody jest czytelna i zrozumiała, formułowana jasnym językiem, pozbawionym hermetycznych branżowych zwrotów, które mogą dezinformować, oraz czy wycofanie zgody przez podmiot danych jest równie łatwe jak jej wyrażenie. Należy również ocenić, czy stosowany system umożliwia weryfikację wieku użytkownika. Dopuszczalne stało się bowiem przetwarzanie danych dzieci w wieku powyżej 16. roku życia na podstawie ich zgody w celu świadczenia im bezpośrednio usług społeczeństwa informacyjnego (świadczonych na odległość, drogą elektroniczną i na indywidualne żądanie odbiorcy usług – np. bankowość internetowa, sklepy internetowe, sprzedaż aplikacji mobilnych).

Po piąte konieczny był przegląd klauzul informacyjnych stosowanych przy zbieraniu danych oraz ocena konieczności uzupełnienia ich o nowe wymagane elementy. Ogólne rozporządzenie o ochronie danych (w art. 13 i 14 rozporządzenia) wprowadziło wymóg przekazania podmiotowi danych znacznie większego pakietu informacji o przetwarzaniu jego danych i przysługujących mu uprawnieniach. W stosunku do poprzedniego stanu prawnego niektóre z obowiązkowych informacyjnych zostały rozszerzone, inne dodane

[570] Zob. M. Byczkowski, *Lista kontrolna ABI*, Biuletyn Administratorów Bezpieczeństwa Informacji: Ochrona Danych Osobowych 2000, nr 2.
[571] Szerzej zob. M. Byczkowski, *Przygotowanie ABI do nowej funkcji inspektora ochrony danych*, Informacja w administracji publicznej 2017, nr 1

po raz pierwszy. I tak należy zwrócić uwagę na obowiązek poinformowania nie tylko o celu przetwarzania danych, ale też wskazać jego podstawa prawna. Nie wystarcza już pouczenie o prawie dostępu do danych, korekty i sprzeciwu wobec ich przetwarzania, ale wymaga się też informacji o prawie do cofnięcia zgody, jeżeli jest ona podstawą przetwarzania, a także o prawie wniesienia skargi do organu nadzorczego. Oznaczenie administratora danych należy uzupełnić też dane kontaktowe IOD, jeżeli został powołany. Obligatoryjne stało się również poinformowanie o profilowaniu podmiotu danych i konsekwencjach zautomatyzowanych decyzji dla praw tej osoby. Zwiększenie zakresu informacji, które należy przekazać osobie, której dane dotyczą, wymaga przekonstruowania klauzul informacyjnych stosowanych na formularzach służących do zbierania danych, papierowych i w Internecie. Nie była to jednak prosta zmiana polegająca na dodaniu nowych elementów, ponieważ podanie wymaganych informacji wymagało wcześniejszego ich ustalenia. Przykładowo sprecyzowanie zakładanego okresu przechowywania danych lub kryteriów ustalania tego okresu wymaga określenia kategorii danych, podstaw i celów ich przetwarzania oraz przypisania każdemu z nich właściwego okresu retencji, mającego podstawę prawną. Dane przetwarzane na podstawie zbieżnych celów niekoniecznie podlegają temu samemu okresowi retencji. Rewizję okresów przechowywania danych należało odczytywać jako kolejny nowy obowiązek.

Po szóste wprowadzono wymóg inwentaryzacji wszystkich procesów, w których administrator podejmuje decyzje w sposób zautomatyzowany, w tym – przypadki profilowania.

Po siódme audyt gotowości do wdrożenia procedur powinien był objąć również istnienie wewnętrznej procedury wymiany informacji o incydentach oraz przyjmowania i udzielania odpowiedzi na wnioski i skargi w dziedzinie ochrony danych. Jednym z nowych obowiązków stało się bowiem zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu w terminie do 72 godzin po jego stwierdzeniu i podmiotowi danych (art. 33 i 34 rozporządzenia). Należy zatem ocenić, czy ewentualne naruszenie zostanie wykryte i czy proces ten będzie odpowiednio szybki (do tej pory wykrycie naruszenia ochrony danych zajmowało podmiotom średnio 86 dni)[572].

Po ósme administratorzy, którzy dokonywali transferów danych osobowych poza UE i EOG, musieli zbadać, czy podstawy, na których dotychczas opierali transfery, nie wymagały zmian. Ogólne rozporządzenie o ochronie danych zwiększyło znaczenie m.in. wiążących reguł korporacyjnych (*BCR – Binding Corporate Rules*). To narzędzie transferów zapewniające ochronę danych na odpowiednim i jednolitym poziomie, niezależnym od standardów ochrony danych obowiązujących w państwie trzecim. Administrator danych musi wybrać podstawy transferu adekwatne do skali tych operacji i uwzględnić hierarchię tych podstaw prawnych tak, aby np. nie opierać masowego przekazywania danych na zgodach osób, których dotyczą[573].

[572] *Trustwave Global Security Report*, https://www2.trustwave.com/rs/815-RFM-693/images/2015 TrustwaveGlobalSecurityReport.pdf, s. 23–26, [dostęp: 05.12.2020].

[573] Szerzej na temat wiążących reguł korporacyjnych zob. 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. Por. 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.

Po dziewiąte administratorzy danych musieli dokonać przeglądu bezpieczeństwa własnych systemów ODO pod kątem odpowiedniego zapewnienia bezpieczeństwa fizycznego, organizacyjnego oraz informatycznego[574].

Po dziesiąte wreszcie aby zapewnić wyżej wspomniane bezpieczeństwo, należało nie tyle wdrożyć ogólne środki bezpieczeństwa, ale takie będące rezultatem wniosków płynących z uprzednio przygotowanej analizy ryzyka, z której miały płynąć zalecenia do poziomów zabezpieczeń oraz konkretnych narzędzi.

Zmiany w obowiązkach proceduralnych wynikające z rozporządzenia PE i Rady (UE) 2016/679

Zmiany normatywne, które zaczęły obowiązywać od dnia 25 maja 2018 roku, zakładały zmianę aksjologiczną w podejściu do zarządzania danymi osobowymi.

Po pierwsze należy podkreślić, iż choć RODO nie wymusiło obowiązku posiadania dokumentacji ochrony danych osobowych, nie mniej z uwagi na charakter systemu prawnego ochrony danych osobowych, w szczególności jego kompleksowość i złożoność – zalecanym pozostało opracowanie i wdrożenie w jednostkach organizacyjnych administratorów stosownej dokumentacji. Warto przypomnieć, że na bazie przepisów obowiązujących do dnia 24 maja 2018 roku, wymaganymi dokumentami były co najmniej: (a) Polityka Bezpieczeństwa Danych Osobowych, oraz (b) Instrukcja Zarządzania Systemem Informatycznym Służącym do Przetwarzania Danych Osobowych. Aktualnie, jedynie art. 24 ust. 2 RODO wspomina o właściwym – jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania – wdrożeniu odpowiednich polityk ODO, przy czym choć przepis choć nie wprowadza wymogu posiadania fizycznej (papierowej) formy dokumentu to niewątpliwie takowa jest w praktyce zalecana. Odpowiednie rozumienie przepisu powinno prowadzić do wniosku, iż opracowanie, wdrożenie i bieżące aktualizowanie dokumentacji ODO jest zalecane oraz konieczne w sytuacji zapewnienia bezpieczeństwa, odpowiedniego do charakteru procesu przetwarzania danych w relacji do sytuacji konkretnego administratora. Tym samym praktyka wypracowała standard posiadania fizycznej formy polityk ODO, w szczególności Polityki Ochrony Danych Osobowych (oraz równolegle Instrukcji Zarządzania Systemem Informatycznym Służącym do Przetwarzania Danych Osobowych – jako dokumentu powiązanego z Polityką). Nie da się ukryć, iż praktyka ugruntowała inklinacje do posiłkowania się przy opracowywaniu dokumentacji już nieobowiązującym rozporządzeniem Ministra Administracji i Cyfryzacji z 11 maja 2015 roku w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji[575].

[574] Szerzej zob. M. Byczkowski, *Zabezpieczanie danych osobowych w RODO*, Informacja w administracji publicznej 2017, nr 2.

[575] Szerzej zob. (a) *Dokumentacja administratora bezpieczeństwa informacji*, red. J. Forysiak, B. Piwowarczyk-Kowalewska, PRESSCOM, Wrocław 2015, (b) *Dokumentacja ochrony danych osobowych. Praktyczny przewodnik krok po kroku,* red. I. Kuc, wyd. Difin S.A., Warszawa 2016, (c) A. Cieniak, *Kompletna dokumentacja z instrukcją zgłoszenia do GIODO,* RBDO, Warszawa 2015, (d) *Dokumentacja administratora bezpieczeństwa informacji*, red. J. Forysiak, B. Piwowarczyk-Kowalewska, PRESSCOM, Wrocław 2015, (e) I. Ruszczyk, *Wzorcowe instrukcje ochrony danych osobowych*, Ośrodek Doradztwa i Doskonalenia Kadr, Gdańsk 1999.

Po drugie, choć zmiany dotyczą wielu aspektów działalności jednostek organizacyjnych, odnosząc się jedynie do wybranych zmian wyrażających się m.in. poprzez: (a) rozszerzenie zakresu przedmiotowego definiowanych terminów, (b) wprowadzenie domniemania zwięzłej, przejrzystej, łatwo dostępnej i zrozumiałej formy kierowania informacji, w szczególności do dzieci, (c) ustanowienie nowych kategorii profilowania, współadministrowania, rejestrowania czynności przetwarzania, (d) zmianę zasad przekazywania informacji pozyskanych w sposób inny niż od osoby, której dane dotyczą, (e) ustanowienie międzynarodowej współpracę na rzecz ochrony danych osobowych, (f) reformę funkcjonowania organów nadzorczych, (g) stabilizacje wykładni przepisów (ustanowienie Europejską Radę Ochrony Danych), należy skonstatować, iż zmiany wprowadziły szereg nowych obowiązków dla administratorów danych. Najważniejszym *novum* jest to, iż administratorzy danych zostali zobowiązani do przyjęcia koncepcji *risk based approach* – która zakłada, że im większe jest ryzyko związane z przetwarzaniem danych, tym większy powinien być zakres obowiązków ciążących na administratorze danych. W konsekwencji wewnętrzny system ochrony danych osobowych w konkretnej jednostce organizacyjnej, musi być projektowany z uwzględnieniem rodzaju przedsiębiorstwa (wielkości, zasięgu operacyjnego, *mergingu*[576], itp.) i zawierać takie nowe elementy implementacyjne w zakresie środków technicznych i organizacyjnych, które dają gwarancje spełnienia m.in. wymogów:

- dokonywania oceny ryzyka, w tym konieczność dokonywania oceny skutków przetwarzania (*privacy impact assessment*), a w konsekwencji domyślnej ochrony danych – zarówno na etapie projektowania systemu, jak i jego eksploatacji;
- dokonywania rejestru czynności związanych z przetwarzaniem danych (zamiast rejestrowania zbiorów danych);
- raportowania naruszenia bezpieczeństwa danych do administracyjnego organu nadzorczego, bez zbędnej zwłoki, a jeżeli jest to wykonalne, nie później niż w czasie 72h po stwierdzeniu naruszenia;
- „pseudonimizacji" i „anonimizacji" danych osobowych, tj. przetwarzania w sposób uniemożliwiający przypisanie ich do zidentyfikowanej lub możliwej do zidentyfikowania osoby, bez użycia dodatkowych informacji;
- wprowadzenia kontroli systemu na profilowaniem, tj. działaniem o charakterze zautomatyzowanego zbierania i przetwarzania danych, które pozwalają bezpośrednio lub pośrednio zidentyfikować osobę (stworzyć profil) poddawaną profilowaniu, w szczególności w oparciu o osobiste preferencje;
- spełnienia rozszerzonego obowiązku informacyjnego, w szczególności poprzez wprowadzenie znacznie większej ilości klauzul (*check box*);
- realizacji prawa do przenoszenia danych, czy prawa do bycia zapomnianym,
- powołania Inspektora Ochrony Danych,
- dotyczących przetwarzania danych w formule transgranicznej czy danych osobowych dzieci.

[576] Zob. Oświadczenie w sprawie wpływu połączeń przedsiębiorstw na prywatność, przyjęte 19 lutego 2020 r., Europejska Rada Ochrony Danych.

Po trzecie, przy całej kompleksowości reformy systemu danych osobowych, należy zauważyć, że nie uległa *de facto* zmianie konieczność spełniania wymogów: posiadania prawidłowej dokumentacji (w zakresie wymaganym), wdrożenia systemu bezpieczeństwa danych osobowych, przeprowadzenia szkoleń dla pracowników przetwarzających dane osobowe, audytu i ewaluacji systemu bezpieczeństwa danych osobowych.

Dokumentacja – uwagi ogólne

Reforma regulacji pranych ochrony danych osobowych, w zakresie dokumentacji, wprowadziła zmodyfikowany tryb prowadzenia polityk. Pomimo braku obowiązku dokumentacyjnego ustawodawca europejski nałożył na administratorów danych szereg wymogów, których spełnianie winno znaleźć odzwierciedlenie w formie zapisu lub opisu, dopuszczając możliwość jego prowadzenia jedynie w formie elektronicznej (np. Rejestr czynności przetwarzania danych osobowych).

Należy jednak pamiętać, że wyjątkiem na mapie generalnego zniesienia obowiązku prowadzenia dokumentacji, jest przepis art. 31 ust. 4 ustawy z dnia 14 grudnia 2018 roku o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości. Zgodnie z normą, administrator definiowany jako podmiot przetwarzający dane w celu rozpoznawania, zapobiegania, wykrywania i zwalczania czynów zabronionych, w tym zagrożeń dla bezpieczeństwa i porządku publicznego, a także wykonywania tymczasowego aresztowania, kar, kar porządkowych i środków przymusu skutkujących pozbawieniem wolności – a więc każdy z definicji administratora określonej w art. 4 ust. 1 wyżej przywołanej ustawy – jest zobowiązany jest do opracowania i wdrożenia polityki ochrony danych osobowych, uwzględniającej sposób dokumentowania zastosowanych przez niego niezbędnych technicznych i organizacyjnych środków, odpowiadającej charakterowi, zakresowi, kontekstowi i celom przetwarzania oraz ryzyku naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia.

Nowe zasady nie wyeliminowały zarówno dotychczas nagromadzonego dorobku praktyki wdrożeń systemów ochrony danych osobowych, jak i dorobku orzecznictwa oraz doktryny, w szczególności zważywszy, iż fundament reżimu prawnego ochrony danych (tj. podstawa międzynarodowo-prawna) pozostał nie zmieniony. Stąd dorobek oraz doświadczenie wypracowane na podstawie wcześniejszego prawa w znacznej mierze nadal służą jako odnośnik dla tworzenia wewnętrznych systemów ochrony danych na podstawie nowych przepisów albo wprost pozostają w zastosowaniu. Jak wspomniano wcześniej, pierwotnie wymogi posiadania dossier ochrony danych osobowych, jak również realne wdrożenie zasad oraz procedur bezpieczeństwa z nich wynikających[577], płynęły wprost z przepisów implementowanej polską

[577] Należy zaznaczyć, iż poprawność dokumentacji ochrony danych osobowych, jako elementu polityki zarządzania bezpieczeństwem informacji Administratora Danych, jak również poprawność stanu wdrożenia wymaganych prawem procesów zabezpieczeń przetwarzania danych osobowych, może być stwierdzona w ramach specjalnie dedykowanych działań podzielonych (tu przykładowo) na następujące etapy: (1) audyt stanu zgodności z prawem przetwarzania danych osobowych, (2) wnioski poadytowe, (3) opracowanie/aktualizacja dokumentacji ochrony danych osobowych, (4) formalna implementacja dokumentacji ochrony danych osobowych, (5) wdrożenie procedur bezpieczeństwa danych osobowych wynikających z polityki oraz instrukcji, (6) przeprowadzenie

ustawą z 29 sierpnia 1997 roku o ochronie danych osobowych, dyrektywy 95/45 w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych – w szczególności z kryteriów bezpieczeństwa określonych w § 4 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia informatyczne służące do przetwarzania danych. Brak dokumentacji, a w rezultacie pozostawanie w stanie nieprzestrzegania prawa, stwarzało ryzyko odpowiedzialności karnej, cywilnej oraz administracyjnej zarówno administratora danych (kierownika jednostki organizacyjnej), jak i podmiotu przetwarzającego dane osobowe (tzw. procesora). Aktualnie to nie sam brak dokumentacji w wersji fizycznej (papierowej, analogowej), ale pozostawanie w stanie nieprzestrzegania zasad ochrony danych osobowych rodzi odpowiedzialność prawną. Jednakże aby jednostka organizacyjna przestrzegała owe zasady, powinny być one ujęte w poprawnie opracowanej i upublicznionej formie dostępnej dla każdego, kto przetwarza dane osobowe w jednostce organizacyjnej. Stąd, mimo braku nakazu prawnego, posiadanie dokumentacji systemu ochrony danych osobowych, tworzącej kręgosłup systemu przetwarzania danych osobowych u danego administratora danych, w obliczu nowych obowiązków i drastycznie podwyższonych kar, stało się tym bardziej niezbędne. Trudno bowiem wyobrazić sobie prawidłowe funkcjonowanie struktury bezpieczeństwa danych osobowych bez prawidłowego wdrożenia, prowadzenia i aktualizacji stosownej dokumentacji.

Ochrona danych osobowych – zarówno pod rządami starych, jak i nowych przepisów – jest realizowana poprzez zastosowanie środków bezpieczeństwa technicznego, fizycznego, informatycznego i procedur organizacyjnych. System ochrony danych jest nadzorowany przez administratora danych, który zarządza bezpieczeństwem ochrony danych osobowych w celu zapewnienia sprawnego i zgodnego z przepisami prawa wykonywania swoich zadań[578].

Dokumentacja systemu ochrony danych osobowych winna uwzględniać – obok wymogów prawnie określonych – również dorobek dobrych praktyk oraz wytycznych, w tym formułowanych przez organy ochrony danych osobowych. Dokumentacja powinna być formalnie przyjęta oraz implementowana przez administratora danych, tj. organ, jednostkę organizacyjną, podmiot lub osobę decydującą o celach i środkach przetwarzania danych osobowych[579].

relewantnych szkoleń dla pracowników z zakresu obowiązków prawnych związanych z przetwarzaniem danych osobowych, (7) kontrola powdrożeniowa wraz z wnioskami pokontrolnymi.

[578] Administrator danych jest zobowiązany podejmować wszelkie niezbędne działania mające zapobiec zagrożeniom dla bezpieczeństwa danych osobowych, w szczególności takim, jak: (1) sytuacje losowe, w tym nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu, jak np. pożar, zalanie pomieszczeń, katastrofa budowlana, kradzież, włamanie; (2) niewłaściwe parametry środowiska, zakłócające pracę urządzeń elektronicznych (nadmierna wilgotność, zbyt wysoka lub niska temperatura, oddziaływanie pola elektromagnetycznego, itp.); (3) awarie sprzętu lub oprogramowania, niewłaściwe działanie procedur serwisowych w tym przyzwolenie na naprawę sprzętu zawierającego dane osobowe poza siedzibą administratora danych; (4) naruszenie bezpieczeństwa danych przez ich nieautoryzowane przetwarzanie; (5) ujawnienie osobom nieupoważnionym zasad ochrony danych lub danych osobowych; (6) celowe lub przypadkowe rozproszenie danych w sieci publicznej (Internecie) z ominięciem zabezpieczeń systemu lub z wykorzystaniem błędów systemu; (7) zewnętrzne ataki przeprowadzane poprzez sieć publiczną (Internet); (8) naruszenia i nieprzestrzegania zasad określonych w dokumentacji ochrony danych osobowych przez osoby upoważnione do przetwarzania danych

[579] Administrator danych realizuje co najmniej następujące zadania: (1) zapewnia by przetwarzanie danych osobowych było zgodne z prawem; (2) stosuje środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną; (3) nadzoruje opracowanie, prowadzi i aktualizuje dokumentację opisującą sposób przetwarzania danych osobowych, (4) wyznacza Inspektora Ochrony Danych jako osobę odpowiedzialną za bezpieczeństwo przetwarzania danych osobowych; (5) wyznacza Administratora Systemu Informatycznego jako osobę odpowiedzialną za bezpieczeństwo systemów informatycznych służących do przetwarzania danych osobowych; (6) upoważnia osoby, w tym pracowników do przetwarzania danych osobowych, poprzez wydanie im imiennych upoważnień do przetwarzania danych osobowych, indywidualnie określając zakres przetwarzania przez nich danych osobowych odpowiadający zakresowi ich obowiązków; (7) anuluje upoważnienia pracowników (oraz innym osobom)

Z treścią dokumentacji powinni zostać zapoznani wszyscy pracownicy[580] oraz wszystkie osoby mające dostęp – na podstawie upoważnienia[581] – do danych osobowych. Treść dokumentacji powinna również zostać udostępniona podmiotom współpracującym z administratorem danych na podstawie zawartej umowy, w szczególności zleceniobiorcom i dostawcom usług (procesorom).

Dokumentacja ochrony danych osobowych winna być wdrożona na poziomie praktycznych zastosowań, jak również na bieżąco aktualizowana do wymogów środowiska przetwarzania danych (np. zmieniających się norm technicznych i nowych rodzajów zagrożeń)[582]. Przez bezpieczeństwo danych osobowych w szczególności rozumie się zapewnienie ich poufności, integralności, dostępności, rozliczalności, autentyczności, niezaprzeczalności, niezawodności – w rozumieniu norm PN-ISO/IEC 27001. System bezpieczeństwa opierać się bowiem powinien na podejściu procesowym określonym w normie, w oparciu o czterofazowy model „planuj/wykonuj/sprawdzaj/działaj", i winien uwzględniać cztery fazy jak następuje:

1) przygotowanie i wdrożenie systemu, w tym m.in.: określenie zakresu systemu bezpieczeństwa informacji, analiza ryzyka, ocena ryzyka, przygotowanie dokumentacji, przygotowanie wdrożenia, wdrożenie,
2) funkcjonowanie systemu, w tym m.in. monitorowanie bezpieczeństwa informacji, planowanie i przeprowadzanie przeglądów i audytów bezpieczeństwa informacji, rejestracja incydentów, zarządzanie ryzykiem, działania korekcyjne i zapobiegawcze, doskonalenie systemu, nadzór nad dokumentacją i zapisami,
3) zarządzanie ciągłością działania, w tym m.in.: analiza zagrożeń, opracowanie planu ciągłości działania, testowanie planu ciągłości działania, doskonalenie planu ciągłości działania, zastosowanie planu ciągłości działania, przywracanie stanu wyjściowego,

do przetwarzania danych osobowych, poprzez wydanie im imiennych anulacji upoważnień do przetwarzania danych osobowych; (8) prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych; (9) informuje osobę, której dane dotyczą o adresie swojej siedziby i pełnej nazwie, celu zbierania danych, prawie dostępu do treści swoich danych oraz ich poprawiania, dobrowolności albo obowiązku podania danych, z zastrzeżeniem wyjątków przewidzianych w ustawie; (10) określa grupy i rodzaje informacji przetwarzanych, w tym wrażliwe grupy informacji ze względu na ich poufność, integralność i dostępność; (11) określa budynki, pomieszczenia, lub części pomieszczeń tworzących obszar w którym przetwarzane są dane; (12) określa miejsca i czasu przetwarzania, przechowywania, tworzenia i niszczenia informacji; (13) określa rodzaje aplikacji oraz urządzeń komputerowych, które są niezbędne do realizacji zadań; (14) nadzoruje poprawność merytoryczną i adekwatność do celów danych osobowych gromadzonych w zbiorach danych; (15) zapewnia zapoznanie osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych; (16) przygotowuje materiały szkoleniowe z zakresu ochrony danych osobowych i prowadzi szkolenia osób upoważnianych do przetwarzania danych osobowych lub współpracuje w tym zakresie z wyspecjalizowanym podmiotem zewnętrznym; (17) zapewnia użytkownikom stanowiska pracy, umożliwiające bezpieczne i zgodne z prawem przetwarzanie danych osobowych, w tym odpowiedni sprzęt informatyczny; (18) przechowuje dane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania; (19) nadzoruje i dba o zgodne z prawem powierzenie przetwarzania danych osobowych; (20) nadzoruje udostępnianie danych osobowych; (21) prowadzi rejestr czynności przetwarzania, za które odpowiada; (22) współpracuje z organem nadzorczym w ramach wykonywania przez niego swoich zadań, w szczególności na jego żądanie udostępnia mu rejestr czynności przetwarzania w celu monitorowania operacji przetwarzania, (23) podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia zasad bezpiecznego przetwarzania danych osobowych; (24) odpowiada za przeprowadzanie regularnych wewnętrznych audytów przestrzegania przepisów dotyczących ochrony danych.

[580] Bez względu na to czy są pracownikami w rozumienia Kodeksu pracy, osobami zatrudnionymi na podstawie umowy cywilnoprawnej, stażystami, praktykantami, czy wolontariuszami.

[581] Integralną częścią upoważnienia, w przypadku zbioru danych przetwarzanych w systemie informatycznym, o których mowa powyżej jest tzw. przekazanie parametrów uwierzytelniania w systemie (Identyfikator). Osoba upoważniona zobowiązuje się do przetwarzania danych zgodnie z udzielonym upoważnieniem oraz z przepisami ustawy. Naruszenie obowiązków może być podstawą do rozwiązania umowy o pracę w trybie art. 52 ustawy z 26 czerwca 1974r. Kodeks Pracy. Osoba upoważniona do przetwarzania danych osobowych jest zobowiązana do zachowania w tajemnicy danych osobowych i sposobu ich zabezpieczenia również po odwołaniu/anulowaniu upoważnienia, a także ustaniu stosunku pracy/rozwiązaniu umowy/zakończeniu realizacji zadań związanych z przetwarzaniem danych osobowych. Upoważnienie jest ważne do odwołania/anulowania.

[582] Dokumentacja ochrony danych osobowych winna wskazywać przykłady zagrożeń, w tym m.in.: (a) naruszenie bezpieczeństwa danych przez nieautoryzowane ich przetwarzanie, (b) ujawnienie osobom nieupoważnionym zasad ochrony danych stosowanych przez administratora danych, względnie bezpośrednio danych przetwarzanych, w tym również nieumyślne ujawnienie danych osobom przebywającym bez nadzoru lub w pomieszczeniach niedostatecznie nadzorowanych, (c) niewykonywanie kopii zapasowych, (d) przetwarzanie danych osobowych niezgodnie z celem, w tym w szczególności w celach prywatnych, (e) wprowadzanie zmian do systemu informatycznego, w tym np. instalowanie programów bez zgody administratora, Inspektora Ochrony Danych, czy Administratora Systemu Informatycznego, (f) niezabezpieczanie danych osobowych lub systemu informatycznego służącego do ich przetwarzania przed opuszczeniem miejsca pracy lub zakończeniem pracy.

4) doskonalenie systemu, w tym m.in.: przegląd procesu zarządzania bezpieczeństwem, audyt bezpieczeństwa systemu, szkolenie kadry i propagowanie wiedzy o bezpieczeństwie informacji, doskonalenie polityk, procedur, standardów, regulaminów i innych dokumentów systemu[583].

Administrator danych, mający w dyspozycji audyt zagrożeń prywatności, w tym zagrożeń dla bezpieczeństwa przetwarzanych danych osobowych, oraz analizę ryzyka oraz ocenę skutków przetwarzania, powinien podejmować wszelkie możliwe działania konieczne, niezbędne i proporcjonalne do zapobiegania zagrożeniom. Ich opis winien znaleźć odzwierciedlenie w dokumentacji systemu ODO, mającej na celu zapewnienie minimalnych standardów, w tym w szczególności w: (1) Polityce Ochrony Danych Osobowych oraz (2) Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych[584].

Polityka Ochrony Danych Osobowych

Polityka Ochrony Danych Osobowych w zakresie przedmiotowym określa zasady oraz wymogi bezpieczeństwa danych osobowych podczas ich przetwarzania w postaci tradycyjnej (fizycznej/papierowej) oraz z wykorzystaniem systemów elektronicznych. Celem Polityki Ochrony Danych Osobowych jest zapewnienie wymaganych prawem standardów bezpieczeństwa i ochrony danych osobowych przetwarzanych w ramach struktury organizacyjnej administratora danych. Polityka Ochrony Danych Osobowych może być jest elementem szerszej struktury systemu zarządzania bezpieczeństwem informacji (*Information Security Management System*), pozostając kompatybilna z innymi politykami, procedurami, instrukcjami oraz innymi dokumentami wchodzącymi w zakres systemu. Polityka powinna również została opracowana zgodnie ze standardami wynikającymi normy PN-EN ISO/IEC 27001:2017, oraz pozostałymi relewantnymi normami PN-EN ISO/IEC 27002:2014, PN-ISO/IEC 27005:2014, PN-EN/ISO 9001:2015, ISO/IEC 31000:2009, ISO/IEC 31010:2007 (ich zaktualizowanymi wersjami), jak również zaleceniami COBIT IT GOVERNANCE wersja 5, rekomendacjami Komitetu RM ds. cyfryzacji.

Politykę oraz jej aktualizacje zatwierdza administrator danych. Dokumenty wykonawcze służące realizacji Polityki zatwierdza administrator danych oraz Administrator Systemu Informatycznego (w razie jego powołania u administratora danych) oraz w zakresie nadzorczym Inspektor Ochrony Danych. Podstawowe cele Polityki to m.in. (1) rozpoznawanie procesów przetwarzania danych osobowych oraz wprowadzonych zabezpieczeń techniczno-organizacyjnych, (2) zapewnienie poufności, integralności oraz rozliczalności przetwarzanych danych osobowych, (3) uzyskanie niezbędnego poziomu bezpieczeństwa poprzez spełnienie wymagań wynikających z prawa, (4) zapewnieniu wysokiego poziomu bezpieczeństwa w sytuacji

[583] Zob. *Ochrona danych osobowych w praktyce*, red. M. Adamska, Difin S.A., Warszawa 2015.
[584] Zob. T. Cygan, M. Geilke, *Polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym,* PRESSCOM, Wrocław 2011.

przetwarzania danych wrażliwych, (5) podnoszenie świadomości ochrony danych osobowych u osób zaangażowanych w procesy przetwarzania danych.

Zasady określone w Polityce należy stosować się do wszystkich podmiotów upoważnionych do przetwarzania danych osobowych oraz przetwarzających dane osobowe w imieniu i na rzecz administratora danych, w tym wszystkich podmiotów lub osób fizycznych, które współuczestniczą w procesie przetwarzania danych osobowych. Polityka Ochrony Danych Osobowych ma zastosowanie do przetwarzania danych osobowych w zbiorach danych, jak również poza zbiorami danych zwłaszcza w przypadku przetwarzania danych w systemie informatycznym, a w szczególności do: (1) wszelkich istniejących, wdrażanych obecnie lub w przyszłości systemów informacyjnych, w tym prowadzonych w formie tradycyjnej (papierowej), jak ewidencje, kartoteki, skorowidze, księgi, wykazy, akta, zbiory dokumentów, w których przetwarzane są dane osobowe, jak i systemów informatycznych; (2) informacji zawierających dane osobowe, lub przetwarzanych w celu realizacji zadań zleconych; (3) wszystkich nośników magnetycznych, optycznych lub papierowych, na których są lub będą znajdować się informacje zawierające dane osobowe; (4) wszystkich obszarów (budynki, pomieszczenia, części pomieszczeń), w których są lub będą przetwarzane dane osobowe. Polityka Ochrony Danych Osobowych powinna zawierać co najmniej odnośniki uwzględniające takie notyfikacje administratora danych jak:

1) postanowienia ogólne, w tym m.in.: (a) deklaracje ochrony, (b) podstawy prawne, (c) cel Polityki, (d) zakres stosowania i rozpowszechniania, (e) wykaz podstawowych skrótów, (f) wykaz podstawowych definicji, (g) słownik pojęć;
2) opis systemu bezpieczeństwa danych osobowych, w tym m.in. strukturę dokumentów polityki bezpieczeństwa danych osobowych;
3) zestawienie porządku formalno-strukturalnego administratora danych, lub szerzej sektora, w którym operuje jednostka, dla której Polityka jest dedykowana;
4) opis systemu przetwarzania danych osobowych w jednostce organizacyjnej;
5) charakterystyka obowiązków administrator danych;
6) odpowiedzialność za bezpieczeństwo danych osobowych, w tym m.in. (a) Inspektora Ochrony Danych (w razie powołania), oraz (b) Administratora Systemu Informatycznego (w razie powołania).
7) charakterystyka ogólna osób mogących dysponować upoważnieniem do przetwarzania danych osobowych w jednostce organizacyjnej;
8) ewidencja osób upoważnionych do przetwarzania danych w jednostce organizacyjnej;
9) wymogi związane ze znajomością regulacji wewnętrznych oraz relewantnym norm prawa powszechnie obowiązującego;
10) wymogi oceny zgodności;
11) obowiązki i odpowiedzialność pracowników (identyfikowanych również jako osoby zatrudnione na umowy cywilno-prawne, lub odbywające staż/praktykę/wolontariat);

12) deskrypcję infrastruktury przetwarzania danych osobowych, w tym m.in.: (a) wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe, (b) rejestr osób upoważnionych do przetwarzania danych, (b) rejestr czynności przetwarzania (kategorii czynności przetwarzania), (c) ocena skutków przetwarzania, (d) sposób przepływu danych pomiędzy systemami;
13) deskrypcję środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych, w tym m.in.: (a) bezpieczeństwo przetwarzania danych osobowych, (b) środki ochrony fizycznej, (c) środki sprzętowe, informatyczne i telekomunikacyjne, (d) środki organizacyjne;
14) zasady przetwarzania danych w tym – przykładowo – procedurę nadawania i anulowania upoważnień do przetwarzania danych osobowych;
15) model zarządzania usługami zewnętrznymi, w tym m.in. schemat: (a) bezpieczeństwa usług zewnętrznych, (b) powierzania i udostępniania przetwarzania danych osobowych, (c) monitorowania i przeglądu usług podmiotu trzeciego;
16) zasady postępowania w przypadku naruszenia bezpieczeństwa danych osobowych;
17) szablon zarządzania incydentami określający co najmniej procedury: (a) kontroli przetwarzania i stanu zabezpieczenia danych, (b) monitorowania incydentów, (c) postępowania w przypadku naruszenia bezpieczeństwa danych osobowych;
18) przeglądy systemu bezpieczeństwa danych osobowych,
19) modele oceny ryzyka i audytu.

Polityka Ochrony Danych Osobowych, co do zasady, winna zawierać szereg elementów stanowiących uzupełnienie implementacyjne Polityki, względnie wzory poszczególnych dokumentów, wykazów, ewidencji, druków, pism, protokołów – niezbędnych dla prawidłowego wdrożenia i utrzymywania systemu ochrony danych osobowych. Uwzględniając aspekt praktyki kompletowania w/w można wyróżnić następujący zestaw załączników, tu prezentowany z wyszczególnieniem wzorów do wykorzystania przez administratora danych oraz osobno gotowych dokumentów stanowiących element wdrożeniowy Polityki u dedykowanego administratora danych.

Przykładowe elementy wdrożeniowe – dedykowane administratorowi danych na etapie wejścia w życie Polityki

- Rejestr osób upoważnionych do przetwarzania danych osobowych[585],
- Analiza ryzyka,
- Ocena skutków przetwarzania dla danych osobowych,

[585] Ewidencja osób upoważnionych do przetwarzania danych osobowych jest prowadzona przez administratora danych pod nadzorem Inspektora Ochrony Danych i zawiera w szczególności: (a) imię i nazwisko osoby upoważnionej do przetwarzania danych osobowych; (c) zakres upoważnienia do przetwarzania danych osobowych; (d) identyfikator, jeśli osoba upoważniona została zarejestrowana w systemie informatycznym, służącym do przetwarzania danych osobowych; (e) datę nadania i odebrania uprawnień. Przełożeni osób upoważnionych odpowiadają za natychmiastowe zgłoszenie do administratora danych oraz Inspektora Ochrony Danych (w razie powołania) osób, które utraciły uprawnienia dostępu do danych osobowych.

- Rejestr czynności przetwarzania,
- Rejestr kategorii czynności przetwarzania,
- Polityka retencyjna – wykaz okresów przechowywania danych osobowych,
- Procedura obiegu pism, oraz niszczenia akt,
- Opis środków technicznych, fizycznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych, w tym: (a) Opis zabezpieczeń ochrony fizycznej danych osobowych, (b) Opis zabezpieczeń sprzętowych infrastruktury informatycznej i telekomunikacyjnej dla fizycznych elementów Systemu, ich połączeń oraz Systemów operacyjnych, (c) Opis zabezpieczeń technicznych i programowych dla procedur, aplikacji, programów, baz danych i innych narzędzi programowych[586],
- Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe[587],
- Instrukcja kancelaryjna oraz archiwizacyjna[588],
- Instrukcja zarządzania kluczami,
- Instrukcja zarządzania naruszeniami,
- Rejestr podmiotów zewnętrznych (kontrahentów)[589],
- Plan szkolenia wewnętrznego z zakresu zasad ochrony danych osobowych.

Przykładowe wzory

- Upoważnienie do przetwarzania danych osobowych oraz obsługi systemu informatycznego i urządzeń wchodzących w jego skład[590],

[586] Dokument winien zawierać dokładny opis wszystkich środków ochrony fizycznej (w tym technicznej oraz organizacyjnej zastosowanych do każdego ze zbiorów danych traktowanych – z punktu widzenia ochrony – indywidualnie.

[587] Dokument winien wskazywać dokładny obszar przetwarzania danych osobowych, w tym wszystkie lokalizacje faktycznego przetwarzania zarówno fizycznego (np. ewidencje, kartoteki), jak i elektronicznego (serwery, dyski, komputery) z wyszczególnieniem zbiorów przyporządkowanych do miejsce przetwarzania – pełnych adresów, charakterystyki lokalizacji (budynek, kondygnacja, uwarunkowania szczególne).

[588] Organy państwowe oraz państwowe jednostki organizacyjne, organy jednostek samorządu terytorialnego oraz samorządowe jednostki organizacyjne (tu jako administratorzy danych) mają obowiązek zapewnić opracowanie i wdrożenie: (a) instrukcji kancelaryjnej, (b) jednolity rzeczowy wykaz akt, oraz (c) instrukcję w sprawie organizacji i zakresu działania archiwum zakładowego lub składnicy akt (instrukcji archiwacyjnej) – zgodnie z wymogami określonymi w ustawie z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach, ustawie z dnia 20 marca 2015 r. o zmianie ustawy o narodowym zasobie archiwalnym i archiwach oraz rozporządzeniem Prezesa Rady Ministrów z dnia 18 stycznia 2011r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych. Co do zasady instrukcja kancelaryjna winna również obowiązywać w ramach Polityki. Mimo, iż wymóg wdrożenia Instrukcji archiwizacyjnej dotyczy organów publicznych zaleca się wdrożenie tejże – w zgodzie z wymogami ochrony danych – także pozostałym kierownikom jednostek organizacyjnych.

[589] Administrator danych zapewnia aby usługi zewnętrzne były prowadzone wyłącznie zgodnie z wymaganiami bezpieczeństwa przetwarzania danych osobowych, wymaganiami umowy powierzenia oraz wymaganiami prawa powszechnie obowiązującego. Wymagania bezpieczeństwa przetwarzania danych osobowych, zakres usług oraz poziom ich dostarczania należy określić precyzyjnie w umowie świadczenia usług oraz w umowie powierzenia przetwarzania danych osobowych. Poprzez właściwe stosowanie wdrożonych zasad bezpieczeństwa danych osobowych, w szczególności reguł nadawania upoważnień do przetwarzania danych osobowych, administrator danych zapewnia aby użytkownicy nie będący pracownikami stosowali te same zasady bezpieczeństwa przetwarzania danych osobowych co użytkownicy będący pracownikami.

[590] Osoby upoważnione do przetwarzania danych osobowych odpowiedzialne są za: (1) zapoznanie się z przepisami prawa w zakresie ochrony danych osobowych oraz postanowieniami Polityki Ochrony Danych Osobowych i Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych z tym zastrzeżeniem, że fakt zapoznania się z przepisami dotyczącymi ochrony danych osobowych oraz wprowadzonymi i wdrożonymi do stosowania przez administratora danych dokumentami, winien być odnotowany w oparciu o stosowne oświadczenie, (2) stosowanie się do zaleceń administratora danych, Inspektora Ochrony Danych oraz Administratora Systemu Informatycznego w zakresie ich kompetencji, (3) przetwarzania danych osobowych wyłącznie w zakresie ustalonym indywidualnie przez Administratora Danych w pisemnym upoważnieniu i tylko w celu wykonywania przydzielonych obowiązków służbowych, (4) niezwłoczne informowanie administratora danych oraz Inspektora Ochrony Danych (w razie powołania) o wszelkich nieprawidłowościach dotyczących bezpieczeństwa danych osobowych przetwarzanych, (5) ochronę danych osobowych oraz środków wykorzystywanych do przetwarzania danych osobowych przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem, (6) korzystanie z systemów informatycznych w sposób zgodny ze wskazówkami zawartymi w instrukcjach obsługi urządzeń wchodzących w skład systemów informatycznych, (7) zachowanie w tajemnicy danych osobowych oraz przestrzeganie procedur ich bezpiecznego przetwarzania przez cały okres zatrudnienia, a także po ustaniu stosunku pracy lub odwołania z pełnionej funkcji, (8) wszelkie operacje wykonywane w systemach informatycznych przy użyciu nadanego identyfikatora oraz hasła.

- Anulowanie upoważnienia do przetwarzania danych osobowych oraz obsługi systemu informatycznego i urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych,
- Upoważnienie do przebywania w obszarze przetwarzania danych osobowych,
- Oświadczenie pracownika o zobowiązaniu się do przestrzegania zasad ochrony danych osobowych,
- Powołanie Inspektora Ochrony Danych,
- Oświadczenie Inspektora Ochrony Danych,
- Powołanie Administratora Systemu Informatycznego,
- Oświadczenie Administratora Systemu Informatycznego,
- Anulowanie powołania Inspektora Ochrony Danych,
- Anulowanie powołania Administratora Systemu Informatycznego,
- Lista kontrolna do umowy powierzenia,
- Rejestr podmiotów zewnętrznych którym powierzono przetwarzanie danych,
- Wniosek o udostępnienie danych osobowych,
- Informacja dla osoby żądającej wykonania obowiązku informacyjnego.
- Klauzule informacyjne (Obowiązek informacyjny) z art. 13 RODO,
- Klauzule informacyjne (Obowiązek informacyjny) z art. 14 RODO,
- Klauzula informacyjne na stronę internetową (*cookies*),
- Klauzula pracownicza,
- Upoważnienie do reprezentowania administratora danych podczas kontroli organu,
- Protokół przekazania dokumentów,
- Rejestr gości administratora danych,
- Oświadczenie o wzięciu udziału w szkoleniu oraz zobowiązaniu się do przestrzegania przedstawionych w trakcie szkolenia zasad ochrony danych osobowych,
- Umowna klauzula poufności,
- Oświadczenie o zobowiązaniu do zachowania poufności,
- Umowa powierzenia przetwarzania danych osobowych[591],
- Protokół zniszczenia,
- Protokół usunięcia danych osobowych,

[591] Powierzenie przetwarzania danych osobowych może mieć miejsce wyłącznie na podstawie pisemnej umowy powierzenia określającej w szczególności zakres i cel przetwarzania danych. Umowa musi określać również zakres odpowiedzialności podmiotu, któremu powierzono przetwarzanie danych z tytułu niewykonania lub nienależytego wykonania umowy. Powierzenie przetwarzania danych osobowych musi uwzględniać określone. W szczególności podmiot zewnętrzny, któremu ma zostać powierzone przetwarzanie danych osobowych, jest obowiązany przed rozpoczęciem przetwarzania danych do podjęcia środków zabezpieczających danych. W umowach stanowiących podstawę powierzenia przetwarzania danych albo eksploatacji systemu informatycznego lub części infrastruktury należy umieścić zobowiązanie podmiotu zewnętrznego do przestrzegania Polityki Ochrony Danych Osobowych oraz zastosowania odpowiednich środków technicznych i organizacyjnych zapewniających bezpieczeństwo i odpowiedni poziom ochrony danych. Powierzenie przetwarzania danych osobowych nie oznacza zwolnienia z odpowiedzialności administratora danych za zgodne z prawem przetwarzanie powierzonych danych, co wymaga w umowach stanowiących podstawę powierzenia przetwarzania danych, umieszczenia prawa administratora danych do przeprowadzenia kontroli w siedzibie podmiotu zewnętrznego m.in. w zakresie przestrzegania obowiązujących regulacji wewnętrznych, umów i właściwych przepisów prawa. Informacje zawierające dane osobowe powinny być przekazywane uprawnionym podmiotom lub osobom za potwierdzeniem odbioru (np. za pokwitowaniem zdawczo-odbiorczym) lub innym bezpiecznym sposobem, określonym wymogiem prawnym lub umową. Powierzając dane osobowe należy zaznaczyć, że można je wykorzystać zgodnie z przeznaczeniem, dla którego zostały zgromadzone. Monitorowanie usług strony trzeciej powinno być udokumentowane i powinno zawierać informacje o poziomie wykonania usługi, incydentach bezpieczeństwa teleinformatycznego oraz ochrony danych osobowych, śladach audytowych, problemach operacyjnych, awariach, błędach i zakłóceniach.

- Protokół z kontroli/czynności sprawdzających w zakresie ochrony danych osobowych[592],
- Sprawozdanie z audytu zgodności przetwarzania danych osobowych z przepisami[593],
- Protokół z czynności audytowych doraźnych w zakresie ochrony danych,
- Monitorowanie zgodności i harmonogram czynności audytowych doraźnych w zakresie ochrony danych,
- Sprawozdanie z kontroli zgodności przetwarzania danych osobowych – wzór,
- Raport z naruszenia bezpieczeństwa danych osobowych[594],
- Rejestr incydentów i zdarzeń wskazujących na naruszenie bezpieczeństwa danych[595],
- Karta obiegowa,
- Wykaz zmian w Polityce.

[592] Kontrola obejmuje audyt zabezpieczeń technicznych, organizacyjnych i jest przeprowadzana przez podmioty odpowiedzialne za bezpieczeństwo teleinformatyczne (Administrator Systemu Informatycznego) oraz organizacyjne, takie jak dokumentacja, upoważnienia, czy zachowania pracowników w odniesieniu do danych osobowych. Pierwszy etap kontroli przetwarzania i stanu zabezpieczenia danych osobowych obejmuje sprawdzenia dokumentacji, w tym co najmniej w zakresie: (a) zgodności dokumentów bezpieczeństwa danych osobowych z obowiązującymi przepisami, (b) dopuszczeń do przetwarzania danych osobowych (kontrola upoważnień), (c) zapoznania się z przepisami oraz wewnętrznymi dokumentami z zakresu ochrony danych osobowych (kontrola oświadczeń, ewidencji w tym zakresie, zgodności ewidencji z upoważnieniami). Drugi etap ma na celu sprawdzanie stanu faktycznego na podstawie obserwacji oraz wywiadów z pracownikami, w szczególności stosowanie procedur i zasad w praktyce: (a) ustawienie sprzętu komputerowego w pomieszczeniach, (b) sposób przechowywania dokumentów (przechowywanie w sposób uniemożliwiający dostęp do nich osobom nieupoważnionym), (c) sposób niszczenia dokumentów, (d) przestrzeganie procedur związanych z zabezpieczeniem danych w trakcie pracy, (e) zgodność między realnym dostępem do zbiorów danych a upoważnieniami, (f) przestrzegania praw osób, których dane są przetwarzane. Trzeci etap obejmuje sprawdzenie bezpieczeństwa teleinformatycznego, w szczególności: (a) poprawność nadawania/zmieniania/odbierania uprawnień do systemów informatycznych, (b) przestrzeganie zasad rozpoczęcia i zakończenia pracy w systemie, (c) blokowanie systemu podczas opuszczenia stanowiska pracy, (d) ważność odpowiednich upoważnień, (e) stosowanie identyfikatorów i hasła dla użytkowników, (f) zapewnianie przez systemy informatyczne służące do przetwarzania danych osobowych odpowiedniego poziomu ochrony, (g) zabezpieczenia systemowe i fizyczne, (h) tworzenie kopii zapasowych; (i) odnotowywanie przez systemy wszelkich czynności wykonywanych na danych osobowych przez użytkowników, (j) niszczenie zbędnych danych wygenerowanych z systemów. Po zakończeniu kontroli podmiot realizujący kontrolę w porozumieniu z Administratorem Systemu Informatycznego przygotowują sprawozdanie ze sprawdzenia zgodności przetwarzania danych osobowych z przepisami. Sprawozdanie przedstawia się administratorowi danych do akceptacji, a następnie wszystkim innym osobom upoważnionym do przetwarzania danych osobowych.

[593] Polityka Ochrony Danych Osobowych powinna być poddawana przeglądowi w formie audytu przynajmniej raz na rok. W razie istotnych zmian dotyczących przetwarzania danych osobowych administrator danych powinien przeprowadzić przegląd Polityki stosownie do potrzeb. Administrator danych analizuje, czy Polityka i pozostała dokumentacja z zakresu ochrony danych osobowych jest adekwatna do: (a) zmian w obowiązującym prawie, (b) zmian organizacyjnych administratora danych, w tym również zmian statusu osób upoważnionych do przetwarzania danych osobowych, (c) zmian w budowie systemu informatycznego. Kontroli podlega sprzęt, system teleinformatyczny, realizacja zabezpieczeń przez pracowników oraz inne osoby upoważnione do przetwarzania danych osobowych oraz przestrzeganie Polityki. Administrator danych może, stosownie do potrzeb, przeprowadzić wewnętrzny audyt zgodności przetwarzania danych z przepisami o ochronie danych osobowych. Zakres, przebieg i rezultaty audytu dokumentowane są na piśmie w protokole podpisywanym przez administratora danych, Inspektora Ochrony Danych (w razie powołania) i Administratora Systemu Informatycznego. Administrator danych może zlecić przeprowadzenie audytu zewnętrznego przez wyspecjalizowany podmiot.

[594] Naruszeniem bezpieczeństwa danych osobowych jest każdy stwierdzony fakt nieuprawnionego ujawniania danych osobowych, udostępniania lub umożliwiania dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, naruszenia środków ochrony fizycznej lub naruszenia jakiegokolwiek elementu systemu informatycznego. W przypadku stwierdzenia naruszenia zabezpieczenia systemu informatycznego lub zaistnienia sytuacji, która może wskazywać na naruszenie zabezpieczenia danych osobowych, każdy pracownik, lub inna osoba upoważniona do przetwarzania danych jest zobowiązany/a przerwać przetwarzanie danych osobowych i niezwłocznie powiadomić o tym fakcie administratora danych, Inspektora Ochrony Danych i Administratora Systemu Informatycznego, a następnie stosować się do podjętych przez niego decyzji. Administrator lub upoważniona przez niego osoba podejmuje wszelkie działania mające na celu minimalizację negatywnych skutków zdarzenia, wyjaśnienie okoliczności zdarzenia, zabezpieczenie dowodów zdarzenia, umożliwienie dalszego bezpiecznego przetwarzania danych. Odmowa udzielenia wyjaśnień lub współpracy z administratorem danych, Inspektorem Ochrony Danych lub Administratorem Systemu Informatycznego traktowana może być jako naruszenie obowiązków pracowniczych, względnie zobowiązań umownych.

[595] Celem Polityki Ochrony Danych Osobowych jest także minimalizacja skutków wystąpienia incydentów bezpieczeństwa, ograniczenie ryzyka powstania zagrożeń oraz występowania incydentów w przyszłości. Zasady zarządzania incydentami mają zastosowanie zarówno w odniesieniu do danych osobowych przetwarzanych w formie tradycyjnej (kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych), jaki w systemach informatycznych (elektronicznych). Do typowych zagrożeń bezpieczeństwa danych osobowych należą m.in.: (1) brak lub niewłaściwe zabezpieczenia fizyczne pomieszczeń, urządzeń i dokumentów; (2) brak lub niewłaściwe zabezpieczenie sprzętu IT oraz oprogramowania przed wyciekiem, kradzieżą lub utratą danych osobowych; (3) niestosowanie zasad ochrony danych osobowych przez osoby upoważnione w tym: (a) nieprzestrzeganie zasad czystego biurka i ekranu, (b) ochrony haseł, (c) niewylogowywanie się przed opuszczeniem stanowiska pracy, (d) pozostawienie danych w drukarce lub kserokopiarce, (e) niewykonanie kopii zapasowych, (f) prace na danych osobowych w celach prywatnych, (h) nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych osobowych, znajdujących się na dyskach, płytach CD, kartach pamięci oraz wydrukach komputerowych (otwarte szafy, biurka, regały, archiwum niezamykanie pomieszczeń itp.). Do nietypowych incydentów bezpieczeństwa danych osobowych należą m.in.: (1) zdarzenia losowe zewnętrzne: (a) pożar obiektu lub pomieszczenia, (b) zalanie wodą, (c) wybuch gazu, (d) utrata zasilania, (e) uszkodzenie w skutek prowadzonych prac remontowych, (f) wilgotność, (g) nieodpowiednia temperatura, (h) wstrząsy, (i) oddziaływania pola elektromagnetycznego, (j) przeciążenia napięcia, (k) utrata łączności itp.; (2) zdarzenia losowe wewnętrzne: (a) awarie sprzętu komputerowego lub oprogramowania, (b) pomyłki ASI, lub osób upoważnionych do przetwarzania danych, (c) utrata/zagubienie nośników zawierających dane osobowe itp.; (3) umyślne incydenty: (a) nieuprawniony dostęp do systemów informatycznych lub pomieszczeń (włamanie), (b) naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie, (c) modyfikacja danych lub zmiana w strukturze danych bez odpowiedniego upoważnienia, (d) działanie wirusów lub innego szkodliwego oprogramowania, (e) świadome zniszczenie danych, sprzętu, oprogramowania, (f) podmienienie lub zniszczenie nośników z danymi osobowymi, (g) kradzież danych, (h) ujawnienie danych osobowych, lub procedur osobom nieupoważnionym, itp.

Model systemu ochrony danych osobowych obowiązujący w latach 1997 – 2018 w Polsce wymagał ponadto co najmniej takich dokumentów jak:

- Wykaz zbiorów danych osobowych wraz ze wskazaniem programów[596],
- Opis struktury zbiorów danych[597],
- Opis zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między poszczególnymi polami informacyjnymi[598],

Z kolei na gruncie wymogów wprowadzonych art. 31 ust. 4 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, za minimalny zakres dokumentacji ochrony danych, niezbędnych do wdrożenia przed administratora, należy uznać wykaz jak następuje[599]:

- dokumentacja dotyczącą realizacji następujących zadań (art. 31. ust. 3):
  - stosowania się do ogólnych zasad przetwarzania (art. 31 ust. 1),
  - stosowania mechanizmów utrzymywania merytorycznej poprawności danych (art. 31 ust. 2),
  - zapewnienia, aby dane były przetwarzane zgodnie z prawem (art. 13–14),
  - stosowania zasad zautomatyzowanego przetwarzania danych osobowych, w tym profilowania (art. 15),
  - funkcjonowania mechanizmów weryfikacji danych osobowych oraz zasad postępowania po anonimizacji (art. 16–18),
  - stosowania zasad rozróżniania danych osobowych (art. 19–20),
  - funkcjonowania mechanizmów przesyłania lub udostępniania danych innym organom, państwu trzeciemu lub organizacji międzynarodowej (art. 21),
- dokumentacja wskazującą faktyczne lub prawne przyczyny odmowy przekazania informacji lub udostępnienia danych osobie, której dane dotyczą (art. 31. ust. 7),
- dokumentacja wskazującą faktyczne lub prawne przyczyny odmowy lub ograniczenia dostępu do danych (art. 23 ust. 4),
- dokumentacja w zakresie odpowiednich środków technicznych oraz niezbędnych zabezpieczeń stosowanych przy przetwarzaniu danych osobowych w celu realizacji zasad domyślnej ochrony danych i ochrony danych w fazie projektowania (art. 32 ust. 3),

[596] Przykładowe historyczne ujęcie zbiorów danych/rejestrów: (a) pracownicy, stażyści, praktykanci, wolontariusze, (b) członkowie związków zawodowych, (c) osoby ubiegające się o pracę, staż, praktykę, wolontariat, (d) osoby przestępujące do egzaminu, (e) postępowania dyscyplinarne, (f) orzeczenia komisji dyscyplinarnej, (g) skargi i wnioski, (h) sprawy sądowe, (i) podmioty, do których wysyłany jest newsletter, (j) kontrahenci, (k) najemcy, (l) dokumentacja księgowo-finansowa, (m) zapytania ofertowe, (n) rejestr wejść i wyjść pracowników, (o) rejestr gości, (p) rejestr rozmów telefonicznych.

[597] W poszczególnych kolumnach należało wskazać (przykładowo) jak następuję. Kolumna (1) – należało wskazać nazwę zbioru danych. Kolumna (2) należało wskazać podstawę prawną przetwarzania. Kolumna (3) – należało wskazać cel przetwarzania danych. Kolumna (4) – należało wskazać zakres danych przetwarzanych w danym zbiorze. Kolumna (5) – należało wskazać czy zbiór podlega rejestracji. Kolumna (6) – należało wskazać jaki system informatyczny obsługuje dany zbiór danych osobowych. Kolumna (7) – należało wskazać grupę użytkowników uprawnionych do przetwarzania danych osobowych w danym zbiorze danych. Kolumna (8) – należało wskazać lokalizację fizyczną zbioru, zgodnie z wyszczególnionymi w Polityce lokalizacjami. Kolumna 9 – należało wskazać rodzaj zabezpieczenia zbioru danych zgodnie z wyszczególnionymi rodzajami zabezpieczeń. Kolumna 10 – należy wskazać retencję danych poszczególnych zbiorów.

[598] Opis poszczególnych zbiorów miał wskazywać wszystkie pole informacyjne występujące w zbiorze (wraz z opisem ich powiązań), przykładowo: imię i nazwisko, data i miejsce urodzenia, PESEL, obywatelstwo, nazwisko rodowe, imię matki, imię ojca, adres zamieszkania, adres korespondencyjny, numer telefonu, numer fax, adres e-mail, tytuł zawodowy i naukowy, numer członkowski, itp.

[599] Zob. *Kiedy stosujemy ustawę DODO – obowiązki z niej wynikające*, https://odo24.pl/blog-post.co-w-sytuacji-gdy-rodo-nie-ma-zastosowania-czyli-obowiazywanie-przepisow-ustawy-dodo, [dostęp: 17.07.2021].

- porozumienie pomiędzy współadministratorami jeżeli administrator działa w modelu współadministrowania danymi osobowymi (art. 33),
- umowa o powierzeniu danych osobowych do przetwarzania w przypadku powierzania danych osobowych do przetwarzania (art. 34),
- wykaz kategorii czynności przetwarzania (art. 35 ust. 1),
- wykaz kategorii czynności przetwarzania dokonywanych w imieniu administratora, jeżeli występuje w pozycji podmiotu przetwarzającego, o którym mowa w art. 4 pkt 12 (art. 35 ust. 3),
- procedura przeprowadzania oraz wyniki oceny skutków planowanych operacji przetwarzania dla ochrony danych, jeżeli dany rodzaj przetwarzania może skutkować powstaniem wysokiego ryzyka naruszenia praw i wolności osób fizycznych (art. 37 ust. 1),
- procedura oraz protokoły ze zniszczenia informatycznych nośników danych wykorzystywanych do przetwarzania danych osobowych (art. 40),
- wniosek o nadanie uprawnień dostępu do danych osobowych oraz oświadczenie osoby, której wniosek dotyczy, o zobowiązaniu się do zapewnienia bezpieczeństwa danych osobowych (art. 41),
- ewidencja osób upoważnionych do przetwarzania danych osobowych (art. 42),
- oświadczenia osób upoważnionych do przetwarzania danych osobowych dotyczące zapewnienia bezpieczeństwa danych osobowych oraz zachowania w tajemnicy udostępnionych danych osobowych oraz sposobów ich zabezpieczenia (art. 43),
- procedura postępowania z naruszeniami ochrony danych osobowych oraz rejestr naruszeń ochrony danych (art. 44).

Obowiązki, o których mowa w Polityce Ochrony Danych Osobowych, powinny dotyczyć wszystkich pracowników w rozumieniu przepisów ustawy Kodeks Pracy, osoby współpracujące z administratorem danych na podstawie zawartej z nim umowy cywilnoprawnej, w szczególności zleceniobiorców i dostawców usług, przyjmujących zlecenie o dzieło, konsultantów, a także osoby odbywające wolontariat, praktykę lub staż. Tak rozumiany pracownik w szczególności – obok konieczności – przestrzegania zasad wynikających z prawa powszechnie obowiązującego oraz poleceń i wytycznych administratora danych: (1) zobowiązany jest do zapoznania się z przepisami prawa w zakresie ochrony danych osobowych, w tym przepisami Polityki i Instrukcji, (2) może przetwarzać dane osobowe wyłącznie w zakresie ustalonym indywidualnie przez administratora danych i tylko w celu wykonywania powierzonych mu obowiązków, (3) zostaje wyposażony w przypisany mu indywidualny i niepowtarzalny identyfikator użytkownika, niezbędny do pracy w systemie, (4) zobowiązany jest do podpisania oświadczenia o zobowiązaniu do zachowania w tajemnicy danych osobowych oraz sposobach ich zabezpieczenia.

Nieprzestrzeganie zasad ochrony danych osobowych, w tym zasad określonych w Polityce i Instrukcji stanowi naruszenie obowiązków pracowniczych i może być przyczyną

odpowiedzialności porządkowej określonej w ustawie Kodeks Pracy. Pracownik, który dopuści się naruszenia zasad bezpiecznego przetwarzania, w szczególności świadomie udostępni dane osobie nieuprawnionej, może zostać pociągnięty do odpowiedzialności skutkującej rozwiązaniem stosunku pracy bez zachowania okresu wypowiedzenia na podstawie art. 52 ustawy Kodeks Pracy. Jeżeli skutkiem nieprzestrzegania zasad ochrony danych osobowych jest szkoda, sprawca ponosi odpowiedzialność materialną na warunkach określonych w ustawie Kodeks Pracy. Nadto naruszenie zasad ochrony danych może narazić pracownika na odpowiedzialność karną, jak również odpowiedzialność odszkodowawczą na zasadach określonych w ustawie o ochronie danych osobowych oraz w przepisach cywilnych.

Instrukcja Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych

Równoległym dokumentem wchodzącym w zakres struktury ochrony danych w danej jednostce organizacyjnej, w sytuacji obiegu danych w systemach informatycznych, powinna być Instrukcja Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych. Celem Instrukcji jest określenie sposobów zarządzania systemem informatycznym (względnie systemami informatycznymi) wykorzystywanym do przetwarzania danych osobowych, w celu ich zabezpieczenia przed zagrożeniami, w tym zwłaszcza przed ich udostępnieniem osobom nieupoważnionym, nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem. Instrukcja określa obowiązki administratora danych w zakresie zabezpieczenia danych osobowych przetwarzanych w systemie informatycznym służącym do przetwarzania danych osobowych, o których mowa w art. 24 oraz 30 rozporządzenia PE i Rady (UE) 2016/679. Instrukcja winna zawierać co najmniej odnośniki uwzględniające takie notyfikacje administratora danych jak:

1) nadawanie i rejestrowanie (wyrejestrowywanie) uprawnień do przetwarzania danych w systemie informatycznym;
2) metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem (identyfikator, hasło użytkownika, hasło administratora);
3) procedury rozpoczęcia, zawieszenia i zakończenia pracy, przeznaczone dla użytkowników systemu, w tym: (a) tryb pracy na poszczególnych stacjach roboczych, (b) tryb pracy na komputerach przenośnych;
4) przechowywanie elektronicznych nośników informacji zawierających dane osobowe
5) procedura transportu nośników;
6) procedura przechowywania nagrań;
7) sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego;
8) sposób zabezpieczenia systemów przed zdarzeniami losowymi oraz nieprzewidzianymi oddziaływaniami czynników zewnętrznych;
9) zasady i sposób odnotowywania w systemie informacji o udostępnieniu danych;

10) zasady korzystania z sieci publicznej (Internetu);
11) zasady korzystania z poczty elektronicznej;
12) tryb kontroli nad elektronicznym wprowadzaniem, przetwarzaniem i udostępnianiem danych;
13) procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych;
14) tryb aktualizacji oprogramowania;
15) metodologię dziennika Administratora Systemów Informatycznych;
16) procedurę przeprowadzania naprawy urządzeń informatycznych;
17) postępowanie w przypadku stwierdzenia naruszenia bezpieczeństwa systemu informatycznego.

Administrator danych ma m.in. obowiązek zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Uwzględniając charakter działalności administratora danych z konieczność zachowania bezpieczeństwa ich przetwarzania w systemie informatycznym, w tym na odcinkach systemu połączonych z siecią publiczną, administrator wprowadza się odpowiedni, proporcjonalny do zagrożeń oraz posiadanych aktywów informacyjnych poziom zabezpieczeń[600].

Instrukcja winna dokładnie przedstawiać – obok środków ochrony fizycznej opisanych głównie w Polityce – środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej ochrony danych, w tym m.in.: (a) zabezpieczenie dostępu do systemów operacyjnych, w których przetwarzane są dane za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła; (b) zobowiązanie pracowników do okresowej ręcznej zmiany haseł; (c) zastosowanie środków ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity; (d) użycie systemu Firewall do ochrony dostępu do sieci komputerowej; (e) zainstalowanie wygaszaczy ekranów na stanowiskach, na których przetwarzane są dane, czy (f) ustawienie ekranów w sposób uniemożliwiający identyfikacje graficzną i treściową zawartości przez innego użytkownika.

W konsekwencji Instrukcja – podobnie jak Polityka – powinna zawierać szereg szczegółowych procedur, instrukcji, druków, pism, ewidencji – w formie wzorów lub dokumentów

[600] Do reformy wynikającej z RODO bezpieczeństwo przetwarzania danych osobowych w systemie informatycznym odzwierciedlało kategorie poziomów bezpieczeństwa danych. Wyróżniano trzy poziomy bezpieczeństwa systemów informatycznych: (1) podstawowy, (2) podwyższony, (3) oraz wysoki. Poziom co najmniej podstawowy stosowano gdy: jednocześnie w systemie informatycznym nie były przetwarzane dane wrażliwe, oraz żadne z urządzeń systemu informatycznego, służącego do przetwarzania danych osobowych nie było połączone z siecią publiczną. Poziom co najmniej podwyższony stosowano, gdy jednocześnie w systemie informatycznym przetwarzane były dane osobowe wrażliwe, oraz żadne z urządzeń systemu informatycznego, służącego do przetwarzania danych osobowych nie było połączone z siecią publiczną. Poziom wysoki stosowano gdy przynajmniej jedno urządzenie systemu informatycznego, służącego do przetwarzania danych osobowych, połączone było z siecią publiczną. Zob. § 6 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. z 2004 r. Nr 100, poz. 1024).

implementacyjnych, niezbędnych dla prawidłowego wdrożenia i utrzymywania systemu ochrony danych osobowych przez administratora danych, w tym m.in.: (1) Procedurę zarządzania użytkownikami systemu (systemów)[601], (2) Procedurę tworzenia i niszczenia kopii zapasowych[602], oraz w formie wzorów do bieżącej aktualizacji: (1) Powołanie Administratora Systemu Informatycznego, (2) Oświadczenie Administratora Systemu Informatycznego, (3) Anulowanie powołania Administratora Systemu Informatycznego, (4) Oświadczenie o wzięciu udziału w szkoleniu w zakresie wykonywanych zadań w Systemie Informatycznym oraz zobowiązaniu się do przestrzegania przedstawionych w trakcie szkolenia zasad ochrony danych osobowych, (5) Rejestr nośników, (6) Rejestr użytkowników i uprawnień w systemie informatycznym, (7) Przekazanie parametrów uwierzytelniania w systemie, (8) Nadanie uprawnień dostępu w systemie informatycznym, (9) Porozumienie w zakresie oprogramowania, (10) Rejestr incydentów informatycznych, (11) Dziennik Administratora Systemu Informatycznego.

Zadania w zakresie zarządzania i bieżącego nadzoru nad systemem informatycznym administratora danych realizuje Administrator Systemu Informatycznego (w razie powołania)[603].

[601] Dostęp do systemu informatycznego służącego do przetwarzania danych osobowych może uzyskać wyłącznie osoba upoważniona przez administratora danych do przetwarzania danych osobowych, zarejestrowana jako użytkownik w tym systemie przez Administratora Systemu Informatycznego. Rejestracja użytkownika polega na nadaniu identyfikatora i przydzieleniu hasła oraz wprowadzeniu tych danych do bazy użytkowników systemu. Wyrejestrowania użytkownika z systemu informatycznego dokonuje Administrator Systemu Informatycznego na wniosek administratora danych. Wyrejestrowanie następuje poprzez: (a) zablokowanie konta użytkownika do czasu ustania przyczyny uzasadniającej blokadę, lub (b) usunięcie danych użytkownika z bazy użytkowników systemu (wyrejestrowanie trwałe). Identyfikator powinien składać się z co najmniej ośmiu (8) znaków, który jest jednoznacznie powiązany z użytkownikiem. W identyfikatorze pomija się polskie znaki diakrytyczne. Hasło powinno składać się z unikalnego zestawu znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne. Hasło nie może być identyczne z identyfikatorem użytkownika ani jego imieniem lub nazwiskiem. System informatyczny powinien wymuszać zmianę hasła co 30 dni. Administrator danych może, w uzasadnionych sytuacjach, polecić dokonanie zmiany hasła przez użytkownika.

[602] W systemie informatycznym kopie zapasowe wykonywane są ręcznie lub z wykorzystaniem dedykowanej aplikacji. Dostęp do kopii bezpieczeństwa mają tylko administrator danych i Administrator Systemu Informatycznego. Kopie tworzy się na oddzielnych nośnikach informatycznych np. nośnikach optycznych lub zewnętrznych dyskach twardych. Nośniki zawierające kopie zapasowe należy oznaczać jako „nr kopii/miesiąc/rok". Częstotliwość wykonywania kopii. Kopie zapasowe tworzy się: (a) raz w tygodniu – na koniec tygodnia kopię wszystkich danych, które uległy zmianie tego tygodnia, (b) raz w miesiącu – na koniec miesiąca kopię zarówno danych, jak i baz danych aplikacji. Kopie zapasowe przechowuje się w zamkniętym sejfie lub kasetce w innymi pomieszczeniu niż to w którym została wykonana kopia zapasowa. Zabrania się przechowywania kopii zapasowych w pomieszczeniach przeznaczonych do przechowywania zbiorów danych pozostających w bieżącym użytkowaniu; jednocześnie kopie zapasowe muszą być odpowiednio zabezpieczone fizycznie. Kopie zapasowe mogą być przechowywane tylko w tych pomieszczeniach, w których jest zainstalowany system wykrywania włamania. Nośniki zawierające nieaktualne kopie danych, będące poza wykazem cyklicznych kopii, likwiduje się; w przypadku nośników jednorazowych, takich jak płyty CD-R, DVD-R, likwidacja polega na ich fizycznym zniszczeniu w taki sposób, by nie można było odczytać ich zawartości; nośniki wielorazowego użytku, takie jak dyski twarde, dyskietki, płyty CD-RW, DVD-RW, można wykorzystać ponownie do celów przechowywania kopii bezpieczeństwa po uprzednim usunięciu ich zawartości. Nośniki wielorazowego użytku nienadające się do ponownego użycia należy zniszczyć fizycznie.

[603] Administrator Systemu Informatycznego powinien być odpowiedzialny m.in. za: (1) wdrożenie zasad ochrony danych osobowych określonych w Polityce Ochrony Danych Osobowych oraz Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych i dokumentach z nimi związanych; (2) realizację wytycznych administratora danych oraz Inspektora Ochrony Danych w zakresie ochrony danych osobowych przetwarzanych z wykorzystaniem środków informatycznych; (3) prowadzenie dokumentacji systemowej opisującej działania związane z administracją systemów informatycznych, w których przetwarzane są dane osobowe; (4) prowadzenie dokumentacji dotyczącej opisu przepływu danych pomiędzy systemami informatycznymi zastosowanymi w celu przetwarzania danych osobowych oraz udostępnianie jej Inspektorowi Ochrony Danych; (5) umożliwienie przeprowadzenia kontroli przez służby Prezesa Urzędu Ochrony Danych Osobowych; (6) nadzór nad stosowaniem środków zapewniających bezpieczeństwo przetwarzania danych osobowych w systemach informatycznych; (7) zarządzanie systemem informatycznym, w którym przetwarzane są dane osobowe, posługując się hasłem administracyjnym dostępu do wszystkich stacji roboczych i serwerów z pozycji administratora; (8) nadzór nad prawidłowym działaniem mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych; (9) na wniosek administratora danych przydzielenie każdemu użytkownikowi identyfikatora oraz hasła do systemu informatycznego oraz dokonanie ewentualnych modyfikacji uprawnień, a także usuwanie kont użytkowników zgodnie z zasadami określonymi w Instrukcji (przydzielenie identyfikatora oraz hasła do systemu informatycznego może nastąpić wyłącznie w odniesieniu do osoby posiadającej upoważnienie do przetwarzania danych osobowych); (10) podejmowanie działań w zakresie ustalania i kontroli identyfikatorów dostępu do systemu informatycznego; (11) sprawowanie nadzoru nad bezpieczeństwem danych osobowych zawartych na dyskach wymiennych, palmtopach, pamięciach przenośnych i innych nośnikach, a także w komputerach przenośnych; (12) sprawowanie nadzoru nad systemem komunikacji w sieci publicznej poprzez terminale komputerowe administratora danych oraz przesyłanie danych za pośrednictwem urządzeń teletransmisji; (13) instalację i konfigurację oprogramowania systemowego i sieciowego zabezpieczającego dane chronione przed nieupoważnionym dostępem; (14) zarządzanie, sprawowanie nadzoru oraz serwis urządzeń komputerowych pracujących w systemie informatycznym, w tym świadczenie pomocy technicznej dla użytkowników; (15) w sytuacji stwierdzenia naruszenia zabezpieczeń systemu informatycznego alarmowanie administratora danych oraz Inspektora Ochrony Danych o naruszeniu oraz współdziałanie z nimi przy usuwaniu skutków naruszenia; (16) zarządzanie kopiami awaryjnymi konfiguracji oprogramowania systemowego i sieciowego; (17) zarządzanie kopiami awaryjnymi danych (w tym danych osobowych) oraz zasobów umożliwiających ich przetwarzanie; (18) zapewnianie bieżącego monitoringu, ciągłości działania oraz optymalizacji wydajności systemu informatycznego; (19) diagnozowanie zdarzeń i usuwanie awarii urządzeń komputerowych; (20) wykonywanie oraz sprawowanie nadzoru nad wykonywaniem napraw, konserwacją oraz likwidacją urządzeń komputerowych, na których przetwarzane są dane osobowe; (21) wykonywanie oraz sprawowanie nadzoru nad wykonywaniem kopii zapasowych, ich przechowywaniem oraz okresowym sprawdzaniem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu informatycznego; (22) podejmowanie działań służących zapewnieniu niezawodności zasilania komputerów, innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz zapewnieniu bezpiecznej wymiany danych w sieci

Administrator danych poprzez Administratora Systemu Informatycznego, działającego pod nadzorem i w porozumieniu z Inspektorem Ochrony Danych powinien sprawować nadzór nad wprowadzanymi, przetwarzanymi w systemie informatycznym oraz udostępnianymi danymi osobowymi. Stąd system informatyczny winien umożliwiać automatyczne przypisanie wprowadzanych danych użytkownikowi (identyfikatorowi użytkownika), który te dane wprowadza do systemu, oraz sporządzenie i wydrukowanie dla każdej osoby, której dane są przetwarzane w systemie, raportu zawierającego co najmniej: (a) datę pierwszego wprowadzenia danych do systemu administratora danych, (b) identyfikator użytkownika wprowadzającego te dane, (c) źródła danych – w przypadku zbierania danych nie od osoby, której one dotyczą, oraz (d) informacje o odbiorcach danych. W przypadku zapewnienia dostępu do sieci publicznej (Internet), administrator danych zobowiązany jest wdrożyć najwyższe standardy bezpieczeństwa danych[604].

Administrator Systemu Informatycznego odpowiada za bezawaryjną pracę systemu IT, w tym: stacji roboczych, aplikacji serwerowych, baz danych, poczty email. Przegląd i konserwacja systemu informatycznego powinny być wykonywane w terminach określonych przez producentów systemu lub zgodnie z harmonogramem Administratora Systemu Informatycznego, z częstotliwością pozwalającą antycypować zagrożenia[605]. Administrator Systemu Informatycznego odpowiada za aktualizację oprogramowania zgodnie z zaleceniami producentów oraz opinią rynkową co do bezpieczeństwa i stabilności nowych wersji. Naprawy i zmiany w systemie informatycznym przeprowadzane przez zewnętrznego serwisanta prowadzone są pod nadzorem Inspektora Ochrony Danych oraz Administratora Systemu Informatycznego w siedzibie lub poza siedzibą administratora danych, po uprzednim nieodwracalnym usunięciu danych w nich przetwarzanych, a jeśli wiązałoby się to z nadmiernymi utrudnieniami, to po podpisaniu umów powierzenia przetwarzania danych.

---

wewnętrznej i bezpiecznej teletransmisji; (23) identyfikowanie i analizowanie zagrożeń, w tym dokonywanie ocen ryzyka, na które może być narażone przetwarzanie danych osobowych w systemach informatycznych; (24) prowadzenie ewidencji sprzętu i oprogramowania; (25) opiniowanie i wnioskowanie zakupów urządzeń komputerowych, urządzeń sieciowych i serwerowych, oprogramowania komputerowego, sieciowego i serwerowego; (26) instalowanie albo nadzór nad instalacją nowo kupionych urządzeń komputerowych; (27) wprowadzanie zmiany w konfiguracji lokalnych urządzeń komputerowych, lokalnym oprogramowaniu systemowym oraz aplikacyjnym po uzgodnieniu z Inspektorem ochrony Danych; (28) konfigurację i administrowanie oprogramowaniem systemowym na stacjach roboczych, archiwizowanie danych z lokalnych stacji roboczych; (29) współpracę z dostawcami usług, sprzętu sieciowego i serwerowego oraz zapewnienie przestrzegania przepisów dotyczących ochrony danych osobowych; (30) wnioskowanie do administratora danych o wprowadzenie zmian w procedurach bezpieczeństwa i standardach zabezpieczeń.

[604] Przykładowe zasady korzystania z Internetu: (1) użytkownik zobowiązany jest do korzystania z Internetu wyłącznie w celach służbowych, (2) zabrania się zgrywania na dysk twardy komputera oraz uruchamia jakichkolwiek programów nielegalnych oraz plików pobranych z niewiadomego źródła, (3) użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z Internetu, (4) zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hackerskim, lub innym zakazanym przez prawo, (5) zabrania się w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł, (6) przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka) oraz adresu www rozpoczynającego się frazą "https:", (7) należy zachować szczególną ostrożność w przypadku żądania lub prośby podania kodów, PIN-ów, numerów, (8) zaleca się, aby użytkownik podczas przesyłania danych osobowych mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata, (9) nie należy otwierać załączników (plików) w mailach nadesłanych przez nieznanego nadawcę lub podejrzanych załączników nadanych przez znanego nadawcę, (10) nie należy otwierać stron internetowych wskazanych hiperlinkami w mailach, gdyż mogą to być hiperlinki do stron zainfekowanych lub niebezpiecznych, (11) użytkownicy nie mają prawa korzystać z maila w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania, (12) użytkownik nie ma prawa wysyłać wiadomości zawierających dane osobowe dotyczące, (13) przy korzystaniu z Internetu, użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i prawa autorskiego.

[605] Zakres przeglądu systemów informatycznych powinien obejmować: (a) zgodność z wymaganiami prawnymi w zakresie przetwarzania danych osobowych, (b) sprawność warstwy sprzętowej do realizacji wszystkich funkcji niezbędnych z punktu widzenia wykonywanych działań, (c) poprawność funkcjonowania systemu operacyjnego (m.in. analiza dzienników zdarzeń) oraz poprawność konfiguracji pod względem wydajności i bezpieczeństwa, (d) poprawność funkcjonowania aplikacji przetwarzającej dane osobowe, (e) zgodność liczby użytkowników i ich uprawnień ze stanem oczekiwanym, (f) zabezpieczenia systemu informatycznego ze względu na mogące się pojawić zagrożenia (brak zasilania, atak złośliwego oprogramowania, awaria sprzętowa), (g) poprawność funkcjonowania systemu kopii zapasowych.

Użytkownik systemu informatycznego, w którym przetwarzane są dane osobowe zobowiązany jest zawiadomić Administratora Systemu Informatycznego lub Inspektora Ochrony Danych o każdym naruszeniu lub podejrzeniu naruszenia bezpieczeństwa systemu, a w szczególności o: (a) naruszeniu hasła dostępu i identyfikatora, (b) częściowym lub całkowitym braku danych albo dostępie do danych w zakresie szerszym niż wynikający z przyznanych uprawnień, (c) braku dostępu do właściwej aplikacji lub zmianie zakresu wyznaczonego dostępu, (d) wykryciu wirusa komputerowego, (e) zauważeniu elektronicznych śladów próby włamania do systemu informatycznego, (f) znacznym spowolnieniu działania systemu informatycznego, (g) podejrzeniu kradzieży sprzętu komputerowego lub dokumentów zawierających dane osobowe, (h) zmianie położenia sprzętu komputerowego, (i) zauważeniu śladów usiłowania lub dokonania włamania do pomieszczeń lub zamykanych szaf. Administrator Systemu Informatycznego, po otrzymaniu zawiadomienia, powinien niezwłocznie: (a) przeprowadzić postępowanie wyjaśniające w celu ustalenia okoliczności naruszenia ochrony danych osobowych, (b) podjąć działania chroniące system przed ponownym naruszeniem, (c) w przypadku stwierdzenia faktycznego naruszenia bezpieczeństwa systemu sporządzić raport naruszenia bezpieczeństwa systemu informatycznego.

Inspektor Ochrony Danych po zapoznaniu się z raportem, podejmuje decyzję o dalszym trybie postępowania, powiadomieniu właściwych organów oraz podjęciu innych szczególnych czynności zapewniających bezpieczeństwo systemu informatycznego administratora danych bądź zastosowaniu środków ochrony fizycznej. Administrator Systemu Informatycznego zobowiązany jest do informowania Inspektora Ochrony Danych o awariach systemu informatycznego, zauważonych przypadkach naruszenia niniejszej instrukcji przez użytkowników, a zwłaszcza o przypadkach posługiwania się przez użytkowników nieautoryzowanymi programami, nieprzestrzegania zasad używania oprogramowania antywirusowego, niewłaściwego wykorzystania sprzętu komputerowego lub przetwarzania danych w sposób niezgodny z procedurami ochrony danych osobowych.

Niezastosowanie się do procedur określonych w Instrukcji może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, skutkujące rozwiązaniem stosunku pracy bez wypowiedzenia, a także rodzić odpowiedzialność cywilną, oraz karną.

Podsumowanie

Reformy normatywne, które zaczęły obowiązywać od dnia 25 maja 2018 roku, zakładały zmianę aksjologiczną w podejściu do zarządzania danymi. Administratorzy – mając na uwadze pozostawanie w zgodności z prawem – powinni prowadzić system bezpieczeństwa danych osobowych, w tym opracować i wdrożyć wymaganą prawem dokumentację ochrony danych osobowych. Porządek prawny obowiązujący do reformy wynikającej z RODO wymagał

stosownego dossier, tj. Polityki Bezpieczeństwa Danych Osobowych, jak i Instrukcji Zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. Dokumenty te musiały być na bieżąco aktualizowane i dostosowywane m.in. do zmieniających się przepisów prawnych oraz przekształceń faktycznych.

Na zmiany wynikające z wejścia rozporządzenia 2016/679 można patrzeć dwutorowo. Z jednej strony zgodnie z nowym porządkiem prawnym system ochrony danych osobowych, jako kręgosłup zarządzania organizacją, musi być prowadzony w czasie rzeczywistym i odzwierciedlać stan nie z dnia przyjęcia dokumentacji, lecz na bieżąco. Tu należy zauważyć, iż model wdrożeniowy na starych przepisach niestety charakteryzował się brakiem dynamizmu „widzącego" zmiany wewnątrz organizacji. Najczęściej był przyjmowany w kształcie odzwierciedlającym datę wdrożenia. Założenia nowego modelu narzucają konieczność implementacji dynamicznego, inteligentne, adaptującego się modelu ODO, z platformą oceny ryzyka i analizy skutków operacji przetwarzania danych (*risk based approach*), które zwrotnie powinny skutkować każdorazowymi aktualizacji (odzwierciedlanymi w dokumentacji). Tworzenie i prowadzenie systemu ochrony danych osobowych pod rządami nowych przepisów wymaga od administratorów danych więcej świadomości, odpowiedzialności, ale także nakładów, w tym organizacyjnych, kompetencyjnych i finansowych. Przy czym należy założyć, że dwuletnie *vacatio legis* pozwoliło uzyskać czas niezbędny na przygotowanie planu działań dostosowawczych, w tym chociażby przeprowadzenie audytu zgodności systemu ochrony danych osobowych z nowymi przepisami, oraz opracowanie i wdrożenie nowych procedur.

Z drugiej strony RODO nie nakłada obowiązku posiadania dokumentacji ochrony danych osobowych. Jedynie art. 24 ust. 2 RODO wspomina o właściwym – jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania – wdrożeniu odpowiednich polityk ODO, przy czym choć przepis nie wprowadza wymogu posiadania fizycznej (papierowej) formy dokumentu, to niewątpliwie takowa jest w praktyce zalecana. Odpowiednie rozumienie normy powinno prowadzić do wniosku, iż opracowanie, wdrożenie i bieżące aktualizowanie dokumentacji ODO jest zalecane oraz konieczne w sytuacji zapewnienia bezpieczeństwa, odpowiedniego do charakteru procesu przetwarzania danych w relacji do sytuacji konkretnego administratora. Stąd, z uwagi na kompleksowość i złożoność systemu, zalecanym pozostało opracowanie i wdrożenie w jednostkach organizacyjnych administratorów stosownej dokumentacji. Nie uległa przecież zmianie konieczność wdrożenia systemu, przeprowadzenia szkoleń, audytu i ewaluacji. Przy czym aktualnie to nie sam brak dokumentacji w wersji fizycznej (papierowej, analogowej), ale pozostawanie w stanie nieprzestrzegania zasad ochrony danych osobowych, rodzi odpowiedzialność prawną.

Tu należy pamiętać, że przepisy szczegółowe i sektorowe mogą inaczej niż RODO kształtować wymogi dokumentacyjne. I tak wyjątkiem na mapie generalnego zniesienia obowiązku prowadzenia dokumentacji, jest przepis art. 31 ust. 4 ustawy z dnia 14 grudnia 2018 roku o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem

przestępczości, który nakłada na administratorów danych opracowania i wdrożenia polityki ochrony danych osobowych, uwzględniającej sposób dokumentowania zastosowanych przez niego niezbędnych technicznych i organizacyjnych środków, odpowiadającej charakterowi, zakresowi, kontekstowi i celom przetwarzania oraz ryzyku naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia. Oznacza to, że wdrożenie w organizacji wymogów wynikających z przepisów RODO, może nie kończyć procesu związanego z zapewnieniem zgodności z przepisami o ochronie danych osobowych.

Wreszcie należy zauważyć, że nowe zasady nie wyeliminowały zarówno dotychczas nagromadzonego dorobku praktyki wdrożeń systemów ochrony danych osobowych, jak i dorobku orzecznictwa oraz doktryny, w szczególności zważywszy, iż fundament reżimu prawnego ochrony danych pozostał niezmieniony (*vide* przepisy prawa międzynarodowego publicznego). W konsekwencji za nic nadzwyczajnego należy uznać spoglądanie praktyków na uchylone (ale mogące spełniać rolę wspomagającą) kryteria bezpieczeństwa określone w § 4 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia informatyczne służące do przetwarzania danych. Brak dokumentacji analogowej, choć nie oznacza automatycznie pozostawania w stanie nieprzestrzegania prawa, to niewątpliwie stwarza większe ryzyko wejścia w sferę odpowiedzialności karnej, cywilnej oraz administracyjnej zarówno administratora danych (kierownika jednostki organizacyjnej), jak i podmiotu przetwarzającego dane osobowe (tzw. procesora). Nadto po prostu ułatwia utrzymanie prawidłowości funkcjonowania struktury bezpieczeństwa danych osobowych.

ZAKOŃCZENIE

System GDPR nie powstał (choć czasami można odnieść takie wrażenie) 25 maja 2018 roku. Z uwagi na wieloletnie obowiązywanie, obrót społeczno-ekonomiczny, bogate orzecznictwo administracyjne i sądowe, praktykę proceduralno-wdrożeniową, wreszcie dorobek opiniodawczy różnych organów (zarówno unijnych, jak i krajowych) system ODO powinien być traktowany jako odrębna gałąź prawna. Ochrona danych osobowych to żywy system prawny, dostosowujący się do palety barw i odcieni, wynikających z jego stosowania. W Europie to system, który oparł się przede wszystkim o Konwencję nr 108 z 1981 roku, następnie był rozbudowywany zarówno na łonie Rady Europy, prawa wtórnego Unii Europejskiej, wreszcie w przestrzeni normatywnej poszczególnych państw członkowskich (przy czym szersza kategoria prawna, jakim jest prawo do prywatności, jest zdecydowanie starsze, i brało swój początek w państwach skandynawskich już pod koniec XVIII wieku). Stąd za prawidłowy należy uznać pogląd na system GDPR uwzględniający nie tylko porządek prawny wynikający z RODO, lecz oddający wieloletnią strukturę systemu ochrony danych osobowych, i dopiero na jej bazie uwypuklający najważniejsze zmiany wynikające z rozporządzenia 2016/679, oraz przepisów pochodnych. Na tym tle, za wprowadzenie do dużej reformy – niczym papierek lakmusowy oddający zmieniające się potrzeby w tym zakresie –należy uznać także kolejne nowelizacje polskiej ustawy o ochronie danych z 1997 roku.

Mając na względzie powyższe proponuje się spojrzenie dynamiczne – nastawione na analizę najważniejszych zmian – pozwalające w domyśle wczuć się w potrzeby legislacyjne, które z kolei powinny być traktowane jako reakcja na presję społeczno-ekonomiczną, tj. zmieniającego się otoczenia cywilizacyjnego i nowych potrzeb w zakresie zapewnienia ochrony danych osobowych. Wymaga to założenia, że czytelnik dysponuje bazą wyjściową podstawowych, klasycznych instytucji ODO, i jest w stanie odpowiednio nałożyć analizę najważniejszych, wybranych zmian, na całość ewoluującego systemu, wyciągając przy tym stosowane wnioski.

Należy zauważyć, że ochrona danych osobowych po 25 maja 2018 roku, została w warstwie normatywnej i praktycznej w ogóle dostrzeżona. Przykładowo panowała w Polsce opinia/przekonanie, że ustawa z 1997 roku się „nie przyjęła" – co w dużej mierze można potwierdzić. Powszechniejsze było niestosowanie ustawy niż jej stosowanie. Administratorzy najczęściej

wdrażali Politykę Bezpieczeństwa Danych Osobowych dopiero w reakcji na pismo GIODO informujące o planowej kontroli. W tym zakresie dopiero RODO zapewniło równowagę pomiędzy prawami przedsiębiorców a prawami osób, których dane dotyczą.

Wprowadzenie rozporządzenia stało się dobrą okazją do uporządkowania sfery związanej z przetwarzaniem danych osobowych zarówno w instytucjach publicznych, jak i prywatnych, a także w organizacjach pozarządowych czy Kościołach oraz związkach wyznaniowych. Popularnym określeniem stała się tzw. „zgodność z RODO". Wraz z nim nastąpiła niebywała wręcz inflacja różnego typu specjalistów i firm zajmujących się ochroną danych osobowych. Rozporządzenie niejako wymusiło podejście długofalowe nastawione na dostosowanie procesów przetwarzania danych do nowych możliwości technologicznych oraz potrzeb wynikających z nowych zagrożeń. Z tego powodu kwestia ochrony danych osobowych oraz zapewnienie bezpieczeństwa procesom ich przetwarzania nabrało szczególne znaczenia (w dobie globalizacji i powszechnego dostępu do Internetu). Praktyka pokazała, że czułość obywateli, administratorów i inspektorów ochrony danych stała się coraz większa.

Zreformowany system prawny oparty o RODO oraz przepisy pochodne stanowił próbę dostosowania reżimu normatywnego do dokonującego się postępu cywilizacyjnego (w szczególności technologicznego i społecznego). Przy tym należy mieć na uwadze fakt, że zmiany ujawniane w ramach konkretnej gałęzi prawnej muszą mieć swój rytm, dynamikę i zawsze stanowią proces. Unijny model ochrony danych oparty o rozporządzenie 2016/679 (ze wszystkimi konsekwencjami prawnymi przypisanymi do tej formy aktu prawnego) to w dużej mierze *novum* – obok kluczowego zestawu reguł nakazujących stosowanie zasad: (1) celowości (*purpose limitation)*, (2) jakości danych (*accuracy)*, (3) adekwatności (*data minimisation, adequacy)* (4) ograniczenia czasowego (*storage minimisation)*, (5) oraz ochrony (*advanced security*) – wprowadzający szereg nowych instytucji. Wszystko razem wymagało zastosowania całkowicie nowego podejścia do zarządzania jednostką organizacyjną administratora, w warstwie bezpieczeństwa informacji, w tym ochrony danych osobowych. W tym zakresie jedynie holistyczne, kompleksowe, profesjonalne podejście do nowych procedur ochrony danych osobowych mogło zapewnić gwarancje uniknięcia kar administracyjnych w wysokości – co należy podkreślić – do 20 000 000 euro, a w przypadku przedsiębiorstwa – w wysokości do 4 % jego całkowitego rocznego obrotu z poprzedniego roku obrotowego.

Nie można stracić z pola widzenia (choć takie powszechne przekonanie panuje), że unijna reforma ochrony danych osobowych zapoczątkowana w połowie 2016 roku, to nie tylko RODO, ale również inne akty prawne – obowiązujące [jak chociażby: (a) rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725, (b) dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680, (c) ustawa z 10 maja 2018 r. o ochronie danych osobowych, (d) ustawa z dnia 9 maja 2018 r. o przetwarzaniu danych dotyczących przelotu pasażera, (e) ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości], bądź też pozostające w przygotowaniu (jak np. rozporządzenie

ePrivacy). Dotyczy to również nowelizacji podstawowych aktów prawnych (jak np. ustawa z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679). Podobnie rzecz ma się w przypadku konieczności uwzględnienia wszelkiego rodzaju aktów, dokumentów i wydarzeń współkształtujących ustrój ODO od 2018 roku, w tym co najmniej:

1) aktów wykonawczych, takich jak: (a) decyzja wykonawcza Komisji (UE) 2020/969 z dnia 3 lipca 2020 r. określająca przepisy wykonawcze dotyczące inspektora ochrony danych, ograniczeń praw osób, których dane dotyczą, i stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 oraz uchylająca decyzję Komisji 2008/597/WE, (b) decyzja wykonawcza Komisji (UE) 2021/914 z dnia 4 czerwca 2021 r. w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679, (c) decyzja wykonawcza Komisji (UE) 2021/915 z dnia 4 czerwca 2021 r. w sprawie standardowych klauzul umownych między administratorami a podmiotami przetwarzającymi na podstawie art. 28 ust. 7 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 oraz art. 29 ust. 7 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725, (d) decyzja Europejskiego Inspektora Ochrony Danych z dnia 2 kwietnia 2019 r. w sprawie przepisów wewnętrznych dotyczących ograniczenia określonych praw osób, których dane dotyczą, w związku z przetwarzaniem danych osobowych w kontekście czynności wykonywanych przez Europejskiego Inspektora Ochrony Danych, (e) decyzja Europejskiego Inspektora Ochrony Danych z dnia 15 maja 2020 r. w sprawie przyjęcia regulaminu wewnętrznego EIOD, (f) komunikat Komisji do PE i Rady Wzmocniona ochrona, nowe możliwości – wytyczne Komisji dotyczące bezpośredniego stosowania ogólnego rozporządzenia o ochronie danych od dnia 25 maja 2018 r., czy (g) komunikat Komisji do PE i Rady Ochrona danych jako filar wzmacniania pozycji obywateli oraz podejścia UE do transformacji cyfrowej – dwa lata stosowania ogólnego rozporządzenia o ochronie danych.
2) aktów wykonawczych i dokumentów organów ponadkrajowych, których bezpośrednim adresatem jest Polska, takich jak: (a) decyzja wykonawcza Komisji (UE) 2021/914 z dnia 4 czerwca 2021 r. w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679, (b) decyzja wykonawcza Komisji (UE) (UE) 2021/915 z dnia 4 czerwca 2021 r. w sprawie standardowych klauzul umownych między administratorami a podmiotami przetwarzającymi na podstawie art. 28 ust. 7 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 oraz art. 29 ust. 7 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725, (c) Opinia EROD 17/2018 w sprawie projektu wykazu sporządzonego przez właściwy polski organ nadzorczy dotyczącego rodzajów operacji przetwarzania podlegających wymogowi

dokonania oceny skutków dla ochrony danych, (d) Opinia EROD 31/2020 w sprawie projektu decyzji właściwego organu nadzorczego Polski w sprawie zatwierdzenia wymogów akredytacji podmiotu monitorującego przestrzeganie kodeksu postępowania zgodnie z art. 41 RODO.

3) dorobku Europejskiej Rady Ochrony Danych (m.in. wytycznych, zaleceń, opinii, oświadczeń, sprawozdań, dokumentów roboczych, czy not informacyjnych), jako organu – spadkobiercy Grupy Roboczej art. 29, w tym takich dokumentów jak: (1) Wytyczne 5/2021, 4/2021, 3/2021, 2/2021, 1/2021, 10/2020, 9/2020, 8/2020, 7/2020, 6/2020, 5/2020, 04/2020, 03/2020, 2/2020, 1/2020, 5/2019, 4/2019, 3/2019, 2/2019, 1/2019, 4/2018, 3/2018, 2/2018, 1/2018, (2) Zalecenia 02/2021, 01/2021, 2/2020, 01/2020, 01/2019, (3) Wspólne Opinie EROD i EIOD 3/2021, 2/2021, 1/2021, (4) Opinie m.in. 18/2021, 17/2021, 16/2021, 15/2021, 14/2021, 3/2019, 28/2018, 23/2018, (5) Oświadczenia m.in. przyjęte 16 grudnia 2021 r., 18 listopada 2021 r., 5/2021 przyjęte 19 maja 2021 r., 4/2021 przyjęte 13 kwietnia 2021 r., 03/2021 przyjęte 9 marca 2021 r., 2/2021 przyjęte 2 lutego 2021 r., przyjęte 15 grudnia 2020 r., przyjęte 15 grudnia 2020 r., przyjęte 19 listopada 2020 r., przyjęte 16 czerwca 2020 r., przyjęte 16 czerwca 2020 r., przyjęte 2 czerwca 2020 r., przyjęte 19 lutego 2020 r., przyjęte 13 marca 2019 r., 2/2019 przyjęte 13 marca 2019 r., 01/2019 przyjęte 25 lutego 2019 r., przyjęte 27 sierpnia 2018 r., przyjęte 25 maja 2018 r., (6) Dokumenty robocze z 15 grudnia 2020 r. i 20 września 2020 r., (7) Sprawozdania, np. EROD dla LIBE przyjęte 26 lutego 2019 r., (8) Wkłady EROD do konsultacji, np. przyjęty 13 listopada 2019 r., (8) Wystąpienia EROD przed TSUE np. w sprawie C-311/18 (Facebook Ireland i Schrems), przyjęte 9 lipca 2019 r., (9) Noty informacyjne, m.in. przyjęta 15 grudnia 2020 r., 12 lutego 2019 r., 12 lutego 2019 r., (10) dokumenty m.in. Tarcza prywatności UE-USA – Sprawozdanie przyjęte 22 stycznia 2019 r. oraz 12 listopada 2019 r., Strategia na lata 2021–2023, przyjęta 15 grudnia 2020 r.

4) relewantnych orzeczeń sądów wspólnotowych, odnoszących się do standardowych klauzul umownych wykorzystywanych do transferu danych poza EOG: wyroku TSUE z dnia 6 października 2015 r. Maximillian Schrems p-ko Data Protection Commissioner (Schrems I), wyroku TSUE z 16 lipca 2020 r. TSUE w sprawie Data Protection Commissioner przeciwko Facebook Ireland Ltd. i Maximilian Schrems, tzw. Schrems II – które to orzeczenia odpowiednio uchyliły decyzje ustanawiające ramy transferu danych pomiędzy UE a USA: (a) decyzję Komisji z dnia 26 lipca 2000 r. przyjętą na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie adekwatności ochrony przewidzianej przez zasady ochrony prywatności w ramach „bezpiecznej przystani" (Safe Harbour), (b) decyzję wykonawczą Komisji (UE) 2016/1250 z dnia 12 lipca 2016 r. przyjętą na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie adekwatności ochrony zapewnianej przez Tarczę Prywatności (Privacy Shield), co w konsekwencji wymusiło konieczność przyjęcia zestawu dwóch nowych

standardowych klauzul umownych z 4 czerwca 2021 r. pomiędzy administratorami oraz procesorami (decyzja wykonawcza Komisji 2021/914) oraz w ramach powierzeń danych (decyzja wykonawcza Komisji 2021/915).

5) relewantnych orzeczeń sądów wspólnotowych w sprawach doniosłych z uwagi za przedmiot, w tym w szczególności: wyroku TSUE z 5 czerwca 2018 roku, w sprawie C-210/16 uznającym, iż podmiot prowadzący fanpage na Facebooku współadministruje danymi osobowymi razem z Facebookiem, czy wyroku TSUE wydanym 29 lipca 2019 roku wyroku w sprawie C-40/17 uznającym, że podmiot zamieszczający na swojej stronie internetowej ikonkę: „Lubię to" Facebooka, współadministruje danymi osobowymi łącznie z tym podmiotem.
6) relewantnych orzeczeń sądów administracyjnych (w 2018 roku skarg na decyzje lub postanowienia Prezesa UODO było 77, w 2019 roku wniesiono do Wojewódzkiego Sądu Administracyjnego w Warszawie 89 skarg na decyzje lub postanowienia Prezesa UODO, natomiast w 2020 roku wniesiono do WSA w Warszawie 112 skarg na decyzje lub postanowienia Prezesa UODO).
7) publikacji krajowego urzędu nadzoru – Prezesa Urzędu Ochrony Danych Osobowych, w tym takich dokumentów jak: (1) Komunikat Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 czerwca 2019 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony, (2) Komunikat Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 sierpnia 2018 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony; poradników wprowadzających dobre praktyki: (a) Ochrona danych osobowych w szkołach i placówkach oświatowych, (b) Ochrona danych osobowych w kampanii wyborczej, (c) Wskazówki Prezesa Urzędu Ochrony Danych Osobowych dotyczące wykorzystywania monitoringu wizyjnego, (d) Jak rozumieć/stosować podejście oparte na ryzyku?
8) dorobku kompetencyjnego krajowego urzędu nadzoru – Prezesa Urzędu Ochrony Danych Osobowych, w tym: (1) decyzji administracyjnych ogółem (w roku 2020 Prezes Urzędu Ochrony Danych Osobowych wydał 1866 decyzji administracyjnych, tj. o 497 więcej w stosunku do roku 2019, w którym wydanych było 1369 decyzji), (2) skarg (w 2018 roku wpłynęło do PUODO 5565 skarg, z czego przeszło 4550 w okresie od 25 maja do 31 grudnia 2018 r., w 2019 roku wpłynęło 9304 skarg, natomiast w 2020 roku wpłynęły w sumie 6442 skargi), (3) postępowań z naruszeniami (od 25 maja do 31 grudnia 2018 r. UODO dokonał analizy 2 446 zgłoszeń naruszeń pod kątem wystąpienia wysokiego ryzyka naruszenia praw lub wolności osób fizycznych, w 2019 roku Urząd Ochrony Danych dokonał analizy 6039 zgłoszeń naruszeń, a w 2020 roku 7507 zgłoszeń naruszeń), (4) kontroli przestrzegania przepisów o ochronie danych osobowych (od 25 maja 2018 roku do 31 grudnia 2018 roku 32 kontrole, w 2019 roku 98

kontrole, w 2020 roku 12 kontroli – z uwagi na utrudnienia pandemiczne), (5) egzekucji administracyjnej/zapewnienia wykonania decyzji (od 25 maja do 31 grudnia 2018 r. prowadzono egzekucję administracyjną 50 decyzji administracyjnych zawierających nałożony na strony nakaz (obowiązek) do wykonania o charakterze niepieniężnym, w 2019 roku prowadzonych było 99 postępowań, z których 52 zostały zakończone, w tym 42 wydaniem decyzji administracyjnej, przy czym w 2019 roku prowadzona była egzekucja administracyjna 118 decyzji administracyjnych zawierających nałożony na strony nakaz (obowiązek) do wykonania o charakterze niepieniężnym, w 2020 roku Prezes UODO prowadził działania egzekucyjne w stosunku do 100 decyzji administracyjnych, z których 98 zawierało nałożony na strony nakaz do wykonania (obowiązek o charakterze niepieniężnym), zaś 2 nałożyły na strony administracyjne kary pieniężne), (6) uprzednich konsultacji (w 2018 roku do PUODO wpłynęły 2 wnioski o przeprowadzenie uprzednich konsultacji, w 2019 roku do Urzędu wpłynęło 5 wniosków, a w 2020 roku 3 wnioski), (7) kodeksów postępowań w ramach realizacji zadania z art. 57 ust. 1 lit. m RODO, w zw. z art. 40 ust. 1–5 RODO (w 2018 roku przeprowadzono dwa warsztaty dla podmiotów zainteresowanych stworzeniem kodeksu postępowania, w 2019 roku odbyło się 20 indywidualnych spotkań z autorami kodeksów, przy czym złożono 1 wniosek o zatwierdzenie projektu kodeksu, natomiast w 2020 roku 4 organizacje złożyły do Prezesa UODO wnioski o zatwierdzenie projektu kodeksu postępowania)[606].

Analizując kolejne sprawozdania roczne Prezesa Urzędu Ochrony Danych Osobowych można zarysować pewne tendencje. Przykładowo odkąd stosowane jest RODO wzrosła liczba skarg na administratorów. W 2017 roku, czyli jeszcze przed RODO, było ich około 2,9 tys., a już w 2018 roku złożono ich ponad 5,5 tys., w 2019 roku nieco ponad 9,3 tys., a w roku 2020 – 6,4 tys. Wzrosła też liczba zgłaszanych przez administratorów naruszeń ochrony danych osobowych i przeprowadzanych kontroli. W 2019 roku UODO otrzymał ponad 6 tys. zgłoszeń naruszeń, natomiast w całym 2020 roku wpłynęło ich łącznie ponad 7,5 tys. Wreszcie w ostatnich trzech latach odnotować należy znaczny wzrost liczby wpływających do UODO pytań prawnych dotyczących stosowania RODO.

To może świadczyć o znaczącym podniesieniu świadomości obowiązywania systemu GDPR, a także samego jego charakteru normatywnego oraz praktycznego, w szczególności obowiązków z niego wynikających. Ponadto o wykładniczym przyroście liczby podmiotów zaangażowanych w obsługę system ochrony danych osobowych. Administratorzy danych, Inspektorzy Ochrony Danych, jak i sami obywatele zaczęli sami identyfikować problemy i poszukiwać ich rozwiązań. Lawinowo wzrosła liczba nie tylko podmiotów zainteresowanych prawidłowością przetwarzania danych osobowych w własnych jednostkach organizacyjnych,

[606] Zob. (a) *Sprawozdanie z działalności Prezesa Urzędu Ochrony Danych Osobowych w roku 2018*, Prezes Urzędu Ochrony Danych Osobowych, (b) *Sprawozdanie z działalności Prezesa Urzędu Ochrony Danych Osobowych w roku 2019*, Prezes Urzędu Ochrony Danych Osobowych, (c) *Sprawozdanie z działalności Prezesa Urzędu Ochrony Danych Osobowych w roku 2020*, Prezes Urzędu Ochrony Danych Osobowych.

ale także przedsiębiorców i ekspertów profesjonalnie zajmujących świadczeniem usług wsparcia. Temat ochrony danych osobowych stał się modny i przedostał się z poziomu wyłącznie eksperckiego, do sfery przekazów medialnych i popularnonaukowych. Wszystko zadziałało inkluzyjnie, zasysając do sfery GDPR, nieznaną wcześniej liczbę osób z jednej strony działających i zajmujących się zawodowo sferą ODO, z drugiej strony chcących się po prostu zabezpieczyć przed niekorzystnymi skutkami odpowiedzialności wynikającej z niewłaściwego obchodzenia się z danymi osobowymi (np. przed karami).

Ponad dwadzieścia lat funkcjonowania ustawy, podobnie jak cztery dodatkowe lata obowiązywania RODO, to okres który usprawiedliwia dokonywanie ocen i ewaluacji. Chodzi nie tylko o dostrzeżenie i opisanie najważniejszych zmian, ale przede wszystkim uchwycenie tendencji, podstawowych trendów w tej przestrzeni. Niezbędne jest także uwzględnienie najważniejszych wydarzeń, relewantnych dla jakości systemu GDPR. Wreszcie celem samym w sobie jest odpowiedź na pytanie czy faktycznie, realnie udało się kolejnymi reformami wzmocnić system ochrony danych osobowych. Czy udało się wyjść z martwego pola prawa, które choć obowiązywało, to w dużej mierze stosowane było albo wyrywkowo (na czas kontroli), albo punktowo (w zakresie wygodnym dla administratorów) albo po prostu z „przymrużeniem oka". Czy aktualny model GDPR prawidłowo odpowiedział na wyzwania cywilizacyjne w tym zakresie. Osobną, dodatkową kwestią jest także reakcja na pandemię.

Niewątpliwe model GDPR kształtowany w praktyce od 2018 roku cechuje się całą paletą nowych lub wzmocnionych instytucji prawnych, mających na celu wzmocnienie ochrony danych osobowych. Ich charakterystyka została wnikliwie zaprezentowana i przeanalizowana. Największą wadą systemu jest jednak to, że struktura GDPR jest cały czas dość skomplikowana dla zwykłych jego użytkowników, a podmioty przetwarzające dane na dużą skale korzystają z tego faktu. Oznacza to, że administratorzy (szczególnie ci znaczący) skonsumowali nowe przepisy w taki sposób, że suma jest równa zero, czyli że choć może jest większa świadomość istnienia przepisów i konieczności zapewnienia ochrony danych, jest nominalnie więcej poszczególnych działań i zaangażowania – to realnie nie ma więcej prywatności, a nawet być może jest jej mniej (z uwagi właśnie – paradoksalnie – na te wszystkie działania, które trzeba było podjąć aby kontynuować swoją dotychczasową działalności). Podmioty zajmujące się przetwarzaniem danych, aby spełnianie nowych wymogów prawnych nie odbywało się kosztem ich swobody działalności, muszą wykazywać się podwójną spostrzegawczością i zapobiegliwości, pozwalająca na takie używanie warstwy normatywnej, która faktycznie przeradza się w praktyczne korzystanie z nadanych praw.

Należy pamiętać, że wdrożenie w organizacji wymogów wynikających z przepisów RODO nie kończy procesu związanego z zapewnieniem zgodności ze standardami ochrony danych osobowych. W systemie prawnym funkcjonuje bowiem szereg aktów prawnych, które uzupełniają ogólne rozporządzenie o przepisy sektorowe, regulujące przetwarzanie danych w określonych branżach. Oznacza to, że organizacje, które w ramach prowadzonej

przez siebie działalności przetwarzają dane, muszą zweryfikować, czy nie czynią tego w warunkach przepisów sektorowych traktowanych jako *lex specialis* wobec RODO, jako *lex generalis*. Dopiero prawidłowe wdrożenie i stosowanie przepisów obu przestrzeni daje gwarancje pozostawania w prawie.

Należy uznać, że system ODO obowiązujący od 2018 roku jest stosunkowo młody, przechodzi przez okres adaptacji praktycznej, swoistych prób i błędów, a jego adresaci cały czas się go uczą. Przykładem może być rosnąca lawinowo liczba zapytań administratorów danych do Prezesa Urzędu Ochrony Danych Osobowych (np. dot. zagadnienia szyfrowania danych złośliwym oprogramowaniem typu „ransomware").

Odpowiedź czy nowy model GDPR odpowiedział na wyzwania cywilizacyjne nie może być jednoznaczna. Na pierwszy rzut oka wprowadzono nowe narzędzia, które w założeniach miały zwiększyć wachlarz gwarancji wzmacniających prywatność. Czy jednak realnie zwiększyło to poziom ochrony danych osobowych. Czy osoby, których dane są przetwarzane faktycznie czują większe bezpieczeństwo. W tym zakresie dominują raczej wątpliwości. Stąd można zaryzykować stwierdzenie, że cały arsenał instrumentarium prawnego – choć wymagający znaczącego nakładu sił i środków w zakresie spełnienia wymagań – realnie nie przekłada się na zdecydowanie wyższy poziom ochrony danych. To wszystko implikuje pogląd, że przyszłość systemu GDPR to kolejne nowelizacje, próby reform, czy wręcz projektowania architektury nowych systemów (jak w przypadku RODO). Potwierdza to tylko pierwotną tezę prezentowaną w niniejszej pracy, iż na system ODO należy patrzeć, jak na niekończący się proces. Przepisy cały czas są trochę spóźnione wobec rzeczywistości przetwarzania danych, szczególnie tej cyfrowej. Należy założyć, że zjawisko będzie się pogłębiać, szczególnie w obliczu nowych wyzwań – zapewnienia ochrony danych osobowych w takich obszarach, jak:

- sztuczna inteligencja,
- badania naukowe,
- medycyna i ochrona zdrowia (np. eksperymenty medyczne),
- genetyka,
- bio i nanotechnologia,
- przestępczość cyfrowa i cyberbezpieczeństwo,
- nowe środki komunikacji,
- przestrzeń kosmiczna,
- wyzwania globalne (np. środowiskowe)

Immanentnym elementem zakończenia są podsumowania poszczególnych rozdziałów.

BIBLIOGRAFIA

Akty prawne

Prawo międzynarodowe publiczne i wspólnotowe/unijne

ONZ

Rezolucja Zgromadzenia Ogólnego ONZ z 16.11.2016 w sprawie prawa do prywatności w erze cyfrowej, sygn. A/C.3/71/L.39/Rev.1

OECD

Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, 23.09.1980, C(80)58/FINAL

Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, 11.07.2013, C(2013)79

The OECD Privacy Framework, OECD 2013

Rada Europy

Konwencja Nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych sporządzona w Strasburgu dnia 28 stycznia 1981 r.

Rezolucja (73) 22 z 26.09.1973 r. dotycząca ochrony prywatności jednostek w odniesieniu do elektronicznych banków danych w sektorze prywatnym, Komitet Ministrów Rady Europy

Rezolucja (74) 29 z 20.09.1974 r. dotycząca ochrony prywatności jednostek w odniesieniu do elektronicznych banków danych w sektorze publicznym, Komitet Ministrów Rady Europy

Rekomendacja (1986) 1 z 23.01.1986 r. w sprawie ochrony prywatności w Internecie – wytyczne w sprawie ochrony danych osobowych używanych dla celów zabezpieczeń społecznych, Komitet Ministrów Rady Europy

Rekomendacja R (1999) 5 23.02.1999 r. w sprawie ochrony prywatności w Internecie – wytyczne w sprawie ochrony osób w zakresie gromadzenia i przetwarzania danych osobowych na „infostradach", Komitet Ministrów Rady Europy

Rekomendacja (2010) 13 z 23.11.2010 r. w sprawie ochrony osób w związku z automatycznym przetwarzaniem danych osobowych podczas tworzenia profili, Komitet Ministrów Rady Europy

Unia Europejska/Wspólnoty

Traktat o Unii Europejskiej i Traktat o funkcjonowaniu Unii Europejskiej – wersja skonsolidowana (Dz.Urz. C 326 z 26.10.2012 r., s. 1)

Umowa między Wspólnotą Europejską a Rządem Kanady o przetwarzaniu zaawansowanych informacji o pasażerach oraz zapisu danych dotyczących nazwiska pasażera (Dz.Urz. UE L 82 z 21.3.2006 r., s. 15)

Umowa między UE a Australią o przetwarzaniu i przekazywaniu przez przewoźników lotniczych australijskiej służbie celnej danych PNR pochodzących z UE (Dz.Urz. UE L 213 z 8.8.2008 r.)

Umowa między USA a UE o wykorzystywaniu danych dot. przelotu pasażera (PNR) praz przekazywania takich danych do Departamentu Bezpieczeństwa Wewnętrznego USA (Dz.Urz. UE L 215 z 11.8.2012 r.)

Karta praw podstawowych Unii Europejskiej (Dz.Urz. UE C 326 z 26.10.2012 r., s. 391–407)

Rozporządzenie (WE) Nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych (Dz.Urz. UE L 8 z 12.01.2001r., s. 1–22)

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)

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/794 z dnia 11 maja 2016 r. w sprawie Agencji Unii Europejskiej ds. Współpracy Organów Ścigania (Europol), zastępujące i uchylające decyzje Rady 2009/371/WSiSW, 2009/934/WSiSW, 2009/935/WSiSW, 2009/936/WSiSW i 2009/968/WSiSW (Dz.Urz. UE L 135 z 24.5.2016 r., s. 53–114)

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.Urz. UE L 295 z dn. 21.11.2018, s. 39–98)

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)

Dyrektywa 2001/20/WE Parlamentu Europejskiego i Rady z dnia 4 kwietnia 2001 r. w sprawie zbliżania przepisów ustawowych, wykonawczych i administracyjnych Państw Członkowskich, odnoszących się do wdrożenia zasady dobrej praktyki klinicznej w prowadzeniu badań klinicznych produktów leczniczych, przeznaczonych do stosowania przez człowieka (Dz. Urz. UE L 121 z 1.5.2001, s. 34–44)

Dyrektywa 2002/58/WE z dnia 12 lipca 2002 w sprawie przetwarzania danych osobowych oraz ochrony prywatności w sektorze komunikacji elektronicznej (Dz. Urz. UE L 201 z 31.07.2002 r., s. 37–47)

Dyrektywa Komisji 2003/94/WE z dnia 8 października 2003 r. ustanawiająca zasady i wytyczne dobrej praktyki wytwarzania w odniesieniu do produktów leczniczych stosowanych u ludzi oraz produktów leczniczych stosowanych u ludzi, znajdujących się w fazie badań (Dz. Urz. UE L 262 z 14.10.2003, s. 22–26)

Dyrektywa 2004/82/WE z dnia 29 kwietnia 2004 r. w sprawie zobowiązania przewoźników do przekazywania danych pasażerów (dyrektywa API), (Dz.Urz. UE L 261 z 6.8.2004 r., s. 24–27)

Dyrektywa Komisji 2005/28/WE z dnia 8 kwietnia 2005 r. ustalająca zasady oraz szczegółowe wytyczne dobrej praktyki klinicznej w odniesieniu do badanych produktów leczniczych przeznaczonych do stosowania u ludzi, a także wymogi zatwierdzania produkcji oraz przywozu takich produktów (Dz.Urz. UE L 91 z 9.04.2005, s. 13–19)

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/1535 z dnia 9 września 2015 r. ustanawiająca procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego (Tekst mający znaczenie dla EOG) (Dz.Urz. UE L z 17.09.2015, s. 1–15)

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 (Dz.Urz. UE L 119 z 4.05.2016 r., s. 89–131)

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/681 z dnia 27 kwietnia 2016 r. w sprawie wykorzystywania danych dotyczących przelotu pasażera (danych PNR) w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania (Dz.Urz. UE L 119 z 4.5.2016 r., s. 132–149)

Decyzja nr 1247/2002/WE Parlamentu Europejskiego, Rady i Komisji z dnia 1 lipca 2002 r. w sprawie regulaminu i ogólnych warunków regulujących wykonywanie obowiązków przez Europejskiego Pełnomocnika ds. Ochrony Danych (Dz.Urz. UE L 183 z 12.7.2002 r., s. 1–2)

Decyzja Rady z dnia 18 lipca 2005 r. w sprawie zawarcia Umowy pomiędzy Wspólnotą Europejską a Rządem Kanady o przetwarzaniu danych API/PNR (2006/230/WE) (Dz.Urz. UE L 82 z 21.3.2006 r., s. 14)

Decyzja Rady upoważniająca do rozpoczęcia negocjacji z Japonią w sprawie umowy między Unią Europejską a Japonią o przekazywaniu i wykorzystywaniu danych dotyczących przelotu pasażera (PNR) w celu zapobiegania terroryzmowi i poważnym przestępstwom transgranicznym oraz walki z nimi, 5378/20, Bruksela 4 lutego 2020 r.

Decyzja nr 2008/597/WE Komisji z dnia 3 czerwca 2008 r. w sprawie przyjęcia przepisów wykonawczych w zakresie inspektora ochrony danych zgodnie z art. 24 ust. 8 rozporządzenia (WE) nr 45/2001 o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych (Dz.Urz. UE L 193 z 22.7.2008 r., s. 7–11)

Decyzja wykonawcza Komisji (UE) 2020/969 z dnia 3 lipca 2020 r. określająca przepisy wykonawcze dotyczące inspektora ochrony danych, ograniczeń praw osób, których dane dotyczą, i stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 oraz uchylająca decyzję Komisji 2008/597/WE (Dz.Urz. UEL 213 z 6.7.2020 r., s. 12–22)

Decyzja wykonawcza Komisji (UE) 2021/914 z dnia 4 czerwca 2021 r. w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 (Tekst mający znaczenie dla EOG), (Dz.Urz. UE L 199 z 7.6.2021 r., s. 31–61)

Decyzja wykonawcza Komisji (UE) 2021/915 z dnia 4 czerwca 2021 r. w sprawie standardowych klauzul umownych między administratorami a podmiotami przetwarzającymi na podstawie art. 28 ust. 7 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 oraz art. 29 ust. 7 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 (Tekst mający znaczenie dla EOG), (Dz.Urz. UE L 199 z 7.6.2021 r., s. 18–30)

Rezolucja Parlamentu Europejskiego z dnia 5 maja 2010 r. dotycząca rozpoczęcia negocjacji w sprawie umów dotyczących rejestru nazwisk pasażerów (PNR) ze Stanami Zjednoczonymi, Australią i Kanadą, 2011/C 81 E/12 (Dz.Urz. UE C z 15.3.2011 r.)

Decyzja Europejskiego Inspektora Ochrony Danych z dnia 2 kwietnia 2019 r. w sprawie przepisów wewnętrznych dotyczących ograniczenia określonych praw osób, których dane dotyczą, w związku z przetwarzaniem danych osobowych w kontekście czynności wykonywanych przez Europejskiego Inspektora Ochrony Danych (Dz.Urz. UE L 99I z 10.4.2019, s. 1–7)

Decyzja Europejskiego Inspektora Ochrony Danych z dnia 15 maja 2020 r. w sprawie przyjęcia regulaminu wewnętrznego EIOD (Dz.Urz. UE L 204 z 26.6.2020 r., s. 49–59)

Komunikat Komisji w sprawie globalnego podejścia do przekazywania danych dotyczących przelotu pasażera (PNR) państwom trzecim, KOM(2010) 492 wersja ostateczna, Bruksela 21.09.2010 r.

Komunikat Komisji do PE i Rady Wzmocniona ochrona, nowe możliwości – wytyczne Komisji dotyczące bezpośredniego stosowania ogólnego rozporządzenia o ochronie danych od dnia 25 maja 2018 r., Bruksela, 24.1.2018r. COM(2018) 43 final

Komunikat Komisji do PE i Rady Ochrona danych jako filar wzmacniania pozycji obywateli oraz podejścia UE do transformacji cyfrowej – dwa lata stosowania ogólnego rozporządzenia o ochronie danych [SWD(2020) 115 final], Bruksela, 24.6.2020 r. COM(2020) 264 final

Prawo krajowe/wewnętrzne

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 1997 r. Nr 78, poz. 483 z późn. zm)

Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (t.j. Dz.U. z 2020 r., poz. 256, 695, 1298, 2320, z 2021 r. poz. 54, 187)

Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy (t.j. Dz.U. z 2020 r., poz. 1320)

Ustawa z dnia 26 stycznia 1982 r. Karta Nauczyciela (Dz.U. z 2019 r. poz. 2215 oraz z 2021 r. poz. 4)

Ustawa z dnia 16 września 1982 r. o pracownikach urzędów państwowych (t.j. Dz.U. z 2020 r. poz. 537)

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2016 r., poz. 922)

Ustawa z dnia 16 listopada 2000 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz.U. z 2000 r. Nr 116, poz. 1216)

Ustawa z dnia 3 lipca 2002 r. Prawo lotnicze (Dz.U. z 2002 r. Nr 130, poz. 1112 z późn. zm.)
Ustawa z dnia 22 stycznia 2004 r. o zmianie ustawy o ochronie danych osobowych oraz ustawy o wynagrodzeniu osób zajmujących kierownicze stanowiska państwowe (Dz.U. z 2004 r. Nr 33, poz. 285)
Ustawa z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (t.j. Dz. U. z 2021 r., poz. 576)
Ustawa z dnia 24 sierpnia 2007 r. o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym (Dz.U. z 2007 r. Nr 165, poz. 1170)
Ustawa z dnia 24 sierpnia 2007 r. o zmianie niektórych ustaw w związku z członkostwem Rzeczypospolitej Polskiej w Unii Europejskiej (Dz.U. z 2007 r. Nr 176, poz. 1238)
Ustawa z dnia 12 lutego 2010 r. o zmianie ustawy o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Systemie Informacji Wizowej i ustawy o ochronie danych osobowych (Dz.U. z 2010 r. Nr 41, poz. 233)
Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. z 2010 r. Nr 182, poz. 1228)
Ustawa z dnia 29 października 2010 r. o zmianie ustawy o ochronie danych osobowych oraz niektórych innych ustaw (Dz.U. z 2010 r. Nr 229, poz. 1497)
Ustawa z dnia 16 września 2011 r. o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej, państw trzecich, agencjami Unii Europejskiej oraz organizacjami międzynarodowymi (Dz.U. z 2011 r. Nr 230, poz. 1371)
Ustawa z dnia 9 maja 2018 r. o przetwarzaniu danych dotyczących przelotu pasażera (Dz.U. z 2019r., poz. 1783)
Ustawa z 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz.U. z 2019 r., poz. 1781)
Ustawa z 10 maja 2018 r. o zmianie ustawy o usługach płatniczych oraz niektórych innych ustaw (Dz. U. z 2018 r., poz. 1075)
Ustawa z dnia 3 lipca 2018 r. – Przepisy wprowadzające ustawę – Prawo o szkolnictwie wyższym i nauce (Dz.U. z 2018 r., poz. 1669)
Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r., poz. 1560)
Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. z 2019 r., poz. 125)
Ustawa z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania 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) (Dz.U. z 2019 r., poz. 730)
Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 3 czerwca 1998 r. w sprawie określenia wzorów wniosku o udostępnienie danych osobowych, zgłoszenia zbioru danych

do rejestracji oraz imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych (Dz.U. z 1998r. Nr 80, poz. 522)

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r., w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. z 2004 r. nr 100, poz. 1024)

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 22 kwietnia 2004 r. w sprawie wzorów imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych (Dz.U. z 2004 r. nr 94, poz. 923)

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz. U. z 2008 r. nr 229, poz. 1536)

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 11 maja 2011 r. zmieniające rozporządzenie w sprawie wzorów imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych (Dz.U. z 2011 r. nr 103, poz. 601)

Rozporządzenie Ministra Spraw Wewnętrznych z dnia 24 października 2012 r. w sprawie wymagań technicznych i organizacyjnych dotyczących przekazywania Straży Granicznej informacji przez przewoźników lotniczych (Dz.U. z 2012 r., poz. 1249)

Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 10 grudnia 2014 r. w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji (Dz. U. z 2014 r., poz. 1934)

Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych (Dz. U. z 2015 r., poz. 719)

Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz.U. z 2015 r., poz. 745)

Rozporządzenie Prezydenta Rzeczypospolitej Polskiej z dnia 19 listopada 2015 r. zmieniające rozporządzenie w sprawie nadania statutu Biuru Generalnego Inspektora Ochrony Danych Osobowych (Dz.U. 2015 r., poz. 2020)

Rozporządzenie Ministra Zdrowia dnia 9 listopada 2015 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobów jej przetwarzania, (Dz.U. z 2015 r. poz. 2069)

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 22 maja 2018 r. w sprawie określenia protokołów i formatów danych wykorzystywanych przez przewoźników lotniczych w celu przekazywania danych PNR do Krajowej Jednostki do spraw Informacji o Pasażerach (Dz.U. z 2018 r., poz. 1012)

Rozporządzenie Rady Ministrów z dnia 30 maja 2018 r. w sprawie przetwarzania danych dotyczących przelotu pasażera przez Krajową Jednostkę do spraw Informacji o Pasażerach (Dz.U. z 2018 r., poz. 1148)

Rozporządzenie Ministra Cyfryzacji z dnia 20 września 2018 r. w sprawie kryteriów uznania naruszenia bezpieczeństwa lub integralności sieci lub usług telekomunikacyjnych za naruszenie o istotnym wpływie na funkcjonowanie sieci lub usług (Dz. U. z 2018r., poz. 1830)

Rozporządzenie Ministra Cyfryzacji z dnia 20 września 2018 r. w sprawie wzoru formularza do przekazywania informacji o naruszeniu bezpieczeństwa lub integralności sieci lub usług telekomunikacyjnych, które miało istotny wpływ na funkcjonowanie sieci lub usług (Dz. U. z 2018r., poz. 1831)

Rozporządzenie Rady Ministrów z dnia 31 października 2018 r. w sprawie progów uznania incydentu za poważny (Dz.U. 2018 poz. 2180)

Rozporządzenie Rady Ministrów z 20 marca 2019 r. w sprawie wzoru legitymacji służbowej pracownika Urzędu Ochrony Danych Osobowych (Dz.U. z 2019 r. poz. 697)

Rozporządzenie Prezesa Rady Ministrów z dnia 31 maja 2019 r. w sprawie trybu i sposobu realizacji zadań przez inspektora ochrony danych (Dz.U. z 2019 r., poz. 1041)

Orzecznictwo

Trybunał Konstytucyjny

Wyrok TK z 24.06.1997, sygn. K 21/96, OTK 1997, nr 2, poz. 23

Wyrok TK z 09.06.1998, sygn. K 28/97, OTK 1998, nr 4, poz. 50

Wyrok TK z 21.10.1998, sygn. K 24/98, OTK 1998, nr 6, poz. 97

Wyrok TK z 20.11.2002, sygn. K 41/02, OTK-A 2002, nr 6, poz. 83

Wyrok TK z 11.05.2005, sygn. K 18/04, OTK-A 2005, nr 5, poz. 49

Wyrok TK z 12.12.2005, sygn. K 32/04, OTK-A 2005, nr 11, poz. 132

Wyrok TK z 30.06.2006, sygn. P 10/06, OTK-A 2006, nr 9, poz. 128

Wyrok TK z 23.06.2009, sygn. K 54/07, OTK-A 2009, nr 6, poz. 86

Wyrok TK z 18.07.2011, sygn. K 25/09, OTK-A 2011, nr 6, poz. 57

Wyrok TK z 30.07.2014, sygn. K 23/11, OTK-A 2014, nr 7, poz. 80

Trybunał Sprawiedliwości UE

Wyrok TSUE z 13 maja 2014 r. w sprawie *Google Spain i Google*, (C131/12), ECLI:EU:C:2014:317

Wyrok TSUE z 6 października 2015 r. w sprawie Maximillian Schrems p-ko Data Protection Commissioner, tzw. Schrems I (C-362/14)

Wyrok TSUE z 5 czerwca 2018 roku w sprawie Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein przeciwko Wirtschaftsakademie Schleswig-Holstein GmbH (C-210/16)

Wyrok TSUE z 29 lipca 2019 roku w sprawie Fashion ID GmbH & Co. KG przeciwko Verbraucherzentrale NRW eV, przy udziale: Facebook Ireland Ltd, Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, (C-40/17)

Wyrok TSUE z 16 lipca 2020 r. TSUE w sprawie Data Protection Commissioner przeciwko Facebook Ireland Ltd. i Maximilian Schrems, tzw. Schrems II (C-311/18)

Sąd Najwyższy i sądy powszechne

Wyrok Sądu Najwyższego z dnia 25 października 1995 r. (I PRN 77/95)

Wyrok Sądu Najwyższego z dn. 18 lutego 2015 r. (I PK 171/14)

Wyrok Sądu Najwyższego z dnia 10 grudnia 2012 r. (I PK 147/12)

Wyrok Sądu Najwyższego z 26 lipca 1979 r., (I PR 64/79), OSNC 1980, Nr 1, poz. 17

Wyrok SA w Gdańsku z 15 marca 1996 r. (I ACR 33/96), OSA 1996, Nr 7–8, poz. 31

Sądownictwo administracyjne

Wyrok NSA z 21 lutego 2000 r. (II SA 1785/99)

Wyrok NSA z 19 kwietnia 2000 r. (II SA 2619/99), Wok. 2000, Nr 7, s. 43

Wyrok NSA z dnia 17 października 2000 r. (II SA 1860/00, niepubl.)

Wyrok WSA w Warszawie z 19 sierpnia 2008 r. (II SA/Wa 605/08)

Postanowienie SKO w Olsztynie z 24.6.1999 r., SKO-511–27/99, OSS 2000, Nr 2, s. 74

Postanowienie SKO we Wrocławiu z 8.2.2001 r., SKO 4521/1/01, OSS 2001, Nr 2, s. 38

Strategie, dokumenty, opinie (soft-law)

Unia Europejska/Wspólnoty

Rezolucja Parlamentu Europejskiego z 21.02.1975 r. w sprawie ochrony praw jednostek w odniesieniu do postępu technicznego w dziedzinie automatycznego przetwarzania danych (Dz.U. WE z 1975 r. Nr C 60, s. 48)

Rezolucja Parlamentu Europejskiego z 8.05.1979 r. w sprawie ochrony praw jednostek w odniesieniu do postępu technicznego w dziedzinie automatycznego przetwarzania danych (Dz.U. WE z 1979r. Nr C 140, s. 34)

Rezolucja Parlamentu Europejskiego z 11.11.2010 r. w sprawie globalnego podejścia do przekazywania krajom trzecim danych dotyczących przelotu pasażera (PNR) oraz zaleceń Komisji dla Rady dotyczących upoważnienia do podjęcia negocjacji między Unią Europejską a Australią, Kanadą i Stanami Zjednoczonymi, P7_TA(2010)0397

Rezolucja Parlamentu Europejskiego z dnia 6.07.2011 r. w sprawie całościowego podejścia do kwestii ochrony danych osobowych w Unii Europejskiej, P7_TA(2011)0323 (CELEX: 52011IP0323, Dz. Urz. UE z 2013 r. Nr CE 33, s. 101)

Rezolucja Parlamentu Europejskiego z 12.03.2014 r. w sprawie realizowanych przez NSA amerykańskich programów nadzoru, organów nadzoru w różnych państwach członkowskich oraz ich wpływu na prawa podstawowe obywateli UE oraz na współpracę transatlantycką w dziedzinie wymiaru sprawiedliwości i spraw wewnętrznych (2013/2188(INI), sygn. P7_TA(2014)0230

Komunikat Komisji Europejskiej z 13.09.1990 r. na temat ochrony jednostek w związku z przetwarzaniem danych osobowych we Wspólnocie oraz bezpieczeństwa informacji, COM(90) 314 final, CELEX: 51990DC0314.

Komunikat Komisji Europejskiej z 4.11.2010 r. do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów: „Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej", COM(2010) 609

Komunikat Komisji Europejskiej z 6.05.2015 r. do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, Strategia jednolitego rynku cyfrowego dla Europy, COM (2015) 192 final, CELEX: 52015DC0192

Komunikat Komisji Europejskiej z 25.05.2016 r. do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, „Platformy internetowe i jednolity rynek cyfrowy. Szanse i wyzwania dla Europy", COM(2016) 288 final, CELEX:52016DC0288

Wspólny komunikat Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów z 7.02.2013 r. „Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń", JOIN(2013) 1 final

European Parliament Directorate General for Internal Policies, National programmes for mass surveillance of personal data in EU Member States and their compatibility with EU law, Bruksela 2003

European Parliament, Directorate General For Internal Policies, "The US surveillance programmes and their impact on EU citizens' fundamental rights", PE 474.405, Bruksela 2013

Directorate General for Internal Policies Policy, The US legal system on data protection in the field of law enforcement. Safeguards, rights and remedies for EU citizens, Bruksela 2015

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

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

EDPB Statement: EDPB cooperation on the elaboration of guidelines, przyjęte 16 grudnia 2021 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 03/2021 w sprawie rozporządzenia w sprawie prywatności i łączności elektronicznej, przyjęte 9 marca 2021 r., Europejska Rada Ochrony Danych

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

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

Oświadczenie w sprawie ochrony danych osobowych przetwarzanych w związku z zapobieganiem praniu pieniędzy i finansowaniu terroryzmu, przyjęte 15 grudnia 2020 r., 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 w sprawie interoperacyjności aplikacji służących do ustalania kontaktów zakaźnych, przyjęte 16 czerwca 2020 r., Europejska Rada Ochrony Danych

Oświadczenie w sprawie przetwarzania danych osobowych w kontekście ponownego otwarcia granic w następstwie pandemii COVID-19, przyjęte 16 czerwca 2020 r., Europejska Rada Ochrony Danych

Oświadczenie dotyczące ograniczeń praw osób, których dane dotyczą, w związku z wprowadzeniem stanu wyjątkowego w państwach członkowskich, przyjęte 2 czerwca 2020 r., Europejska Rada Ochrony Danych

Oświadczenie w sprawie wpływu połączeń przedsiębiorstw na prywatność, przyjęte 19 lutego 2020r., Europejska Rada Ochrony Danych

Oświadczenie 3/2019 w sprawie rozporządzenia o prywatności i łączności elektronicznej, przyjęte 13 marca 2019 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 2019r., 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 2019 r., 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 2020 r., 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

Opinia 4/2007 w sprawie pojęcia danych osobowych, WP 136, przyjęta 20 czerwca 2007 r., Grupa robocza art. 29

Opinia 1/2010 w sprawie pojęć „administrator danych" i „przetwarzający", WP 169, przyjęta 16 lutego 2010r., Grupa robocza art. 29

Opinia 07/2010 dotycząca komunikatu Komisji w sprawie globalnego podejścia do przekazywania danych dotyczących przelotu pasażera (PNR) państwom trzecim, WP 178, przyjęta 12 listopada 2010, Grupa robocza art. 29

Opinia 15/2011 w sprawie definicji zgody, WP 187, przyjęta 13 lipca 2011 r., Grupa robocza art. 29

Opinia 02/2012 w sprawie systemów rozpoznawania twarzy w usługach online i usługach komórkowych, WP 192, przyjęta 22 marca 2012 r., Grupa robocza art. 29

Opinia 3/2012 w sprawie zmian sytuacji w dziedzinie technologii biometrycznych, WP 193, przyjęta 27 kwietnia 2012 r., Grupa robocza art. 29

Opinia 01/2014 w sprawie stosowania pojęć konieczności i proporcjonalności oraz ochrony danych w sektorze egzekwowania prawa, WP 211, przyjęta 27 lutego 2014 r., Grupa robocza art. 29

Opinia 06/2014 w sprawie pojęcia uzasadnionych interesów administratora danych zawartego w art. 7 dyrektywy 95/46/WE, WP 217, przyjęta 9 kwietnia 2014 r, Grupa robocza art. 29

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

Working Document on surveillance of electronic communications for intelligence and national security purposes, WP 228, Grupa robocza art. 29

Working Document on the surveillance of electronic communications in the workplace, WP 55, Grupa robocza art. 29

Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU, WP 221, Grupa robocza art. 29

Przyszłość prywatności: Wspólny wkład do Konsultacji Komisji Europejskiej w sprawie ram prawnych dla podstawowego prawa do ochrony danych osobowych, WP 168, Grupa robocza art. 29

Transfer danych osobowych do państw trzecich: Stosowanie art. 26 ust. 2 dyrektywy o ochronie danych do wiążących reguł korporacyjnych dla międzynarodowych transferów danych, WP 74, Grupa robocza art. 29

Dokumenty Prezesa Urzędu Ochrony Danych Osobowych

Jak rozumieć podejście oparte na ryzyku? Poradnik RODO, Podejście oparte na ryzyku, Część 1, maj 2018, Prezes Urzędu Ochrony Danych Osobowych

Jak stosować podejście oparte na ryzyku? Poradnik RODO, Podejście oparte na ryzyku, Część 2, maj 2018, Prezes Urzędu Ochrony Danych Osobowych

Komunikat Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 sierpnia 2018 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony (Monitor Polski z 24 sierpnia 2018 r., poz. 827)

Komunikat Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 czerwca 2019 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony (Monitor Polski z 8 lipca 2019 r., poz. 666)

Ochrona danych osobowych w szkołach i placówkach oświatowych – poradnik, sierpień 2018, Prezes Urzędu Ochrony Danych Osobowych

Ochrona danych osobowych w kampanii wyborczej – poradnik, wrzesień 2018, Prezes Urzędu Ochrony Danych Osobowych

Sprawozdanie z działalności Prezesa Urzędu Ochrony Danych Osobowych w roku 2018, Prezes Urzędu Ochrony Danych Osobowych

Sprawozdanie z działalności Prezesa Urzędu Ochrony Danych Osobowych w roku 2019, Prezes Urzędu Ochrony Danych Osobowych

Sprawozdanie z działalności Prezesa Urzędu Ochrony Danych Osobowych w roku 2020, Prezes Urzędu Ochrony Danych Osobowych

Wskazówki Prezesa Urzędu Ochrony Danych Osobowych dotyczące wykorzystywania monitoringu wizyjnego, czerwiec 2018, Prezes Urzędu Ochrony Danych Osobowych

Inne

Big data, artificial intelligence, machine learning and data protection, Information Commissioner's Office, 4.09.2017

Big Data: A Tool for Inclusion or Exclusion?, Federal Trade Commission 2016

Międzynarodowe Standardy Ochrony Danych Osobowych i Prywatności, Rezolucja Madrycka, 5.11.2009

Rezolucja w sprawie prywatności w fazie projektowania przyjęta przez 32. Międzynarodową Konferencję Rzeczników Ochrony Danych i Prywatności, Jerozolima 2010

Druki zwarte

10 lat ochrony danych osobowych w Polsce, red. Fajgielski P., KUL, Lublin 2008

Abramson J.B., Artertone F.Ch., Orren C.,R., *The Electronic Commonwealth: The Impact of New Media Technologies in Democratic Politics*, Nowy Jork 1988

Adamski A., *Prawo karne komputerowe*, Warszawa 2000

Aktualne problemy rozgraniczenia właściwości sądów administracyjnych i powszechnych, red. Błachucki M., Górzyńska T., Naczelny Sąd Administracyjny, Warszawa 2011

Alberts D.S., Gartska J.J., Hayes R.E., Signori D.A., *Understanding information age warfare*, CCRP, Waszyngton 2001

Alberts D.S., *Information Age transformation. Getting to a 21st century military*, CCRP, Waszyngton 1996

Amerykański system ochrony praw człowieka, red. Jaskiernia J., Toruń 2015

Balicki A., Barta P., Byczkowski M., Gumularz M., Jurczyk M., Kędzierska K., Kowalik P., Litwiński P., Sobczak J., Stępień A., Wociór D., *Ochrona danych osobowych w sektorze publicznym. Z uwzględnieniem ogólnego rozporządzenia unijnego,* wyd. C.H. Beck, Warszawa 2016

Banyś T., Bielak-Jomaa E., Kuba M., Łuczak J., *Prawo ochrony danych osobowych. Podręcznik dla studentów i praktyków,* wyd. Diffin, Warszawa 2016

Banyś, T., Łuczak, J., *Ochrona danych osobowych w praktyce. Jak uniknąć błędów i ich konsekwencji prawnych*, wyd. PRESSCOM, Wrocław 2017

Barta J., Fajgielski P., Markiewicz R., *Ochrona danych osobowych. Komentarz*, Wolters Kluwer, Warszawa 2015

Barta J., Markiewicz R., *Internet a prawo*, Warszawa 1998

Barta J., Markiewicz R., *Ochrona danych osobowych. Komentarz*, Wyd. Zakamycze, Kraków 2001

Barta J., Markiewicz R., *Ustawa o ochronie baz danych. Komentarz*, Wyd. Zakamycze, Kraków 2002

Barta J., Litwiński P., *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2013

Barta P., Litwiński P., *Ustawa o ochronie danych osobowych. Komentarz*, C.H. Beck, Warszawa 2016

Bauer Z., Chudziński E., *Dziennikarstwo i świat mediów*, Oficyna Cracovia, Kraków 1996

Beck U., *Władza i przeciwwładza w epoce globalnej: nowa ekonomia polityki światowej*, przeł. J. Łoziński, Warszawa 2005

Biała Księga. Polska – Unia Europejska. Ochrona danych osobowych, red. Barta J., Markiewicz R., Opracowania i Analizy. Seria: Prawo, Zeszyt 32, Urząd Rady Ministrów, Biuro Pełnomocnika Rządu ds. Integracji Europejskiej oraz Pomocy Zagranicznej, Warszawa 1995

Brin D., *The Transparent Society*, Nowy Jork 2009

Brzeziński P., Opaliński B., Rogalski M., *Gromadzenie i udostępnianie danych telekomunikacyjnych*, Warszawa 2016

Buczkowski K., *Prawnokarna problematyka ochrony danych osobowych*, Instytut Wymiaru Sprawiedliwości, Warszawa 2015

Castells M., Himanen P., *Społeczeństwo informacyjne i państwo dobrobytu*, przeł. M. Penkala, M. Sutowski, Krytyka Polityczna nr 17, Warszawa 2009

Castells M., *Galaktyka Internetu. Refleksje nad Internetem, biznesem i społeczeństwem*, przeł. T. Hornowski, Poznań 2003

Castells M., *Koniec tysiąclecia*, przeł. J. Stawiński, S. Szymański, Warszawa 2009

Castells M., *Siła tożsamości*, przeł. S. Szymański, Warszawa 2009

Castells M., *Społeczeństwo sieci*, przeł. M. Marody, K. Pawluś, J. Stawiński, S.Szymański, Warszawa 2007

Castells M., *The Informational City: Information technology, Economic Restructuring and Urban Regional Process*, Blackwell, Oxford, Cambridge, MA 1989

Chrzczonowicz P., Kwiatkowska-Darul V., Skowroński K., *Społeczeństwo inwigilowane w państwie prawa*, wyd. UMK, Toruń 2003

Cieniak A., *Kompletna dokumentacja z instrukcją zgłoszenia do GIODO,* RBDO, Warszawa 2015

Cygan T., Geilke M., *Polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym,* PRESSCOM, Wrocław 2011

Czajkowska-Matosiuk K., *RODO dla samorządu i administracji. Wzory dokumentów z objaśnieniami*, INFOR PL S.A, Warszawa 2018

Dahl R.A., Stinebrickner B., *Współczesna analiza polityczna*, przeł. P.M. Kazimierczak, Scholar, Warszawa 2010

Dai X., *Digital Revolution and Governance*, Ashgate Publication, Londyn 2000

Decydowanie publiczne, red. Rydlewski, G., Warszawa 2011

Dereń A.M., *Ochrona danych osobowych. Omówienie przepisów Ustawy*, Towarzystwo Naukowe Organizacji i Kierownictwa, Bydgoszcz 1998

Dokumentacja administratora bezpieczeństwa informacji, red. Forysiak J., Piwowarczyk-Kowalewska B., PRESSCOM, Wrocław 2015

Dokumentacja ochrony danych osobowych. Praktyczny przewodnik krok po kroku, red. Kuc I., wyd. Difin S.A., Warszawa 2016

Drozd A., *Ustawa o ochronie danych osobowych. Komentarz. Wzory pism i przepisy*, Lexis Nexis, Warszawa 2008

Dziuba D., *Gospodarki nasycone informacją i wiedzą*, Warszawa 2001

Fajgielski P., *Kontrola przetwarzania i ochrony danych osobowych. Studium teoretyczno-prawne,* Wydawnictwo KUL, Lublin 2008

Fajgielski P., *Ochrona danych osobowych w telekomunikacji – aspekty prawne*, Lubelskie Towarzystwo Naukowe, Lublin 2003

Fajgielski P., *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2018

Fajgielski P., *Prawo ochrony danych osobowych Zarys wykładu*, Wolters Kluwer, Warszawa 2019

Fischer B., Świerczyńska-Głownia W., *Dostęp do informacji ustawowo chronionych, zarządzanie informacją*, Uniwersytet Jagielloński, Kraków 2006

Florini A., *The Third Force: The Rise of Transnational Civil Society*, Nowy Jork 2000

Foucault M., *Filozofia, Historia, Polityka – wybór pism*, Warszawa, Wrocław 2000

Goban-Klas T., *Cywilizacja medialna. Geneza, ewolucja, eksplozja*, Warszawa 2005

Goban-Klas T., *Społeczeństwo informacyjne. Szanse, zagrożenia, wyzwania*, Kraków 1999

Grzelak A., *Ustawa o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości. Komentarz*, C.H. Beck, Warszawa 2019

Grzybczyk K., Auleytner A., Kulesza J., *Prawo w wirtualnych światach*, Difin, Warszawa 2013

Habermas J., *Filozoficzny dyskurs nowoczesności*, przeł. M. Łukaszewicz, Kraków 2000

Habermas J., *Strukturalne przeobrażenia sfery publicznej*, przeł. W. Lipnik, M. Łukaszewicz, Warszawa 2007

Held D., *Democracy and the global order: From the modern state to Cosmopolitan Governance*, Stanford 1995

Held H., McGrew A., Goldblatt D., Perraton J., *Global Transformations: Politics, Economics and Culture*, Stanford 1999

Internet. Prawno-informatyczne problemy sieci, portali i e-usług, red. Szpor G., Wiewiórowski W., CH Beck, Warszawa 2012

Internet – problemy prawne, red. Skubisz R., Lublin 1999

Internet rzeczy. Bezpieczeństwo w Smart city, red. Szpor G., C.H. Beck, Warszawa 2015

Iserzon E., Starościak J., *Kodeks postępowania administracyjnego. Komentarz, teksty, wzory i formularze*, Warszawa 1970

Jabłoński M., Wygoda K., *Dostęp do informacji i jego granice,* Uniwersytet Wrocławski, Wrocław 2002

Jackowski M., *Ochrona danych medycznych*, Wolters Kluwer, Warszawa 2018

Jagielski M., Krasińska M., Litwiński P., Kawczyński P., Wojsyk K., Sieradzka A., Bielak-Jomaa E., Andres K., *Ochrona danych osobowych medycznych*, Warszawa 2016

Jatkiewicz P., *Ochrona danych osobowych Teoria i Praktyka*, Polskie Towarzystwo Informatyczne, Warszawa 2015

Kamińska-Kasjaniuk J., *Metodyka pracy administratora bezpieczeństwa informacji,* wyd. JDS Consulting sp. z o.o. sp.k., Warszawa 2016

Kępa L., *Dane osobowe w firmie. Praktyczny poradnik przedsiębiorcy*, Wyd. I, Difin, Warszawa 2011

Kępa L., *Ochrona danych osobowych*, Difin, Warszawa 2014

Kluszczyński R.W., *Społeczeństwo informacyjne. Cyberkultura. Sztuka multimediów*, wyd. 2, Rabid, Kraków 2002

Kodeks pracy. Komentarz, red. Sobczyk A., Warszawa 2017

Krasuski A., *Chmura obliczeniowa. Prawne aspekty zastosowania*, Warszawa 2018

Krasuski A., Skolimowska D., *Dane osobowe w przedsiębiorstwie*, Warszawa 2007

Krzysztofek M., *Tajemnice zawodowe i ochrona danych osobowych w instytucjach finansowych*, Wolters Kluwer, Warszawa 2015

Krzysztofek K., *Władza i obywatel w społeczeństwie informacyjnym*, Warszawa 1999

Kulesza J., *Międzynarodowe prawo Internetu*, Poznań 2010

Litwiński P., *Ochrona danych osobowych w ogólnym postępowaniu administracyjnym*, wyd. I, Wolters Kluwer, Warszawa 2009

Litwiński P., *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, Wyd. C.H. Beck, Warszawa 2017

Liwszic P., Ochocki T., Pociecha Ł., *Ustawa o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości. Komentarz*, C.H. Beck, Warszawa 2019

Marek, B. Nowakowski, *Ochrona danych osobowych i informacje niejawne w sektorze publicznym*, Wydanie 2, Wydawnictwo C.H. Beck, Warszawa 2015

Mattelart A., *Społeczeństwo informacji*, przeł. J. Mikułowski, Kraków 2004

Maziarz A., *Reguły konkurencji Unii Europejskiej*, C.H. Beck, Warszawa 2019

Mazur M., *Jakościowa teoria informacji*, Warszawa 1970

McLuhan M., *Zrozumieć media. Przedłużenie człowieka*, przeł. N. Szucka, Warszawa 2004

Mednis A., *Prawo a ekonomia. Ochrona danych osobowych w obrocie gospodarczym*, wyd. Stowarzyszenia Absolwentów WPiA UW, Warszawa 2013

Mednis A., *Prawna ochrona danych osobowych,* wyd. SCHOLAR, Warszawa 1995

Mednis A., *Prawo do prywatności a interes publiczny,* Wolters Kluwer, Warszawa 2006

Mednis A., *Ustawa o ochronie danych osobowych*, Wydawnictwo Prawnicze PWN, Warszawa 1999

Mednis A., *Wiążące reguły korporacyjne jako podstawa prawna przekazywania danych osobowych do państwa trzeciego,* Wyd. Stow. Absolwentów WPiA UW, Warszawa 2013

Nahotko M., *Metadane. Sposób na porządkowanie Internetu* wyd. UJ, Kraków 2004

Napierała K., *Prawne aspekty ochrony danych osobowych przetwarzanych w systemach informatycznych*, Dom Wydawniczy ABC, Warszawa 1997

Ochrona danych osobowych. Aktualne problemy i nowe wyzwania, red. Sibiga G., Konarski X., Wolters Kluwer Business, Warszawa 2007

Ochrona danych osobowych – poradnik dla małych i średnich przedsiębiorców, red. P. Sikorski, Polska Agencja Rozwoju Przedsiębiorczości, Warszawa 2017

Ochrona danych osobowych pracowników w świetle rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/678, red. Dörre-Kolasa D., Warszawa 2017

Ochrona danych osobowych, red. Wyrzykowski M. Instytut Spraw Publicznych, Warszawa 1999

Ochrona danych osobowych w Polsce i w Niemczech – koncepcje, praktyka, polityka, Materiały z Konferencji z dn. 10–11.X.1996 r., Fundacja im. Friedricha Naumanna Przedstawicielstwo w Polsce, Wydział Prawa Uniwersytetu Wrocławskiego

Ochrona danych osobowych w praktyce. Jak uniknąć błędów i ich konsekwencji prawnych, red. Kościelska K., Wrocław 2013

Ochrona danych osobowych w praktyce, red. Adamska M., Difin S.A., Warszawa 2015

Ochrona danych osobowych w sieci, red. Blaczkowska B., PRESSCOM, Wrocław 2012

Ochrona danych osobowych w Unii Europejskiej po reformie. Komentarz do rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679, red. Krzysztofek M., Warszawa 2016

Ochrona danych podmiotów objętych prawem pracy i prawem ubezpieczeń społecznych, red. Wyka T., Nerka A., Wolters Kluwer Polska, Warszawa 2012

Ogólne rozporządzenie o ochronie danych osobowych. Komentarz, red. M. Sakowska-Baryła, Warszawa 2018

Ogólne rozporządzenie o ochronie danych osobowych. Wybrane zagadnienia, red. Kawecki M., Osiej T., wyd. C.H. Beck, Warszawa 2017

Petzel J., *Informatyka i prawo. Zagadnienia teorii i praktyki*, Warszawa 2000

Polok M., *Bezpieczeństwo danych osobowych*, Warszawa 2016

Polska i europejska reforma ochrony danych osobowych, red. Bielak-Jomaa, E., Lubasz D., Wolters Kluwer, Warszawa 2016

Porębski L., *Elektroniczne oblicze polityki – demokracja, państwo, instytucje polityczne w okresie rewolucji informacyjnej*, Kraków 2004

Powierzenie przetwarzania osobowych danych medycznych i inne problemy współczesnego prawa medycznego, red. Królikowska-Olczak, M., SERIA, Łódź 2013

Prawna ochrona danych osobowych w Polsce na tle europejskich standardów, red. Szabłowska M., Goździewicz G., Wydawnictwo Dom Organizatora, Toruń 2008

Prawna ochrona danych. Uzasadnienie projektu ustawy przyjętej przez Radę Ministrów 13 sierpnia 1996r., Przegląd Rządowy 1996, nr 10

Prawo gospodarcze. Zagadnienia administracyjnoprawne, red. Gronkiewicz-Waltz H., Wierzbowski M., Warszawa 2015

Prawo Internetu, red. Podrecki P., Warszawa 2007

Prawo procesowe administracyjne, red. Hauser R., Wróbel A., Niewiadomski Z., wyd. 3, Warszawa 2017

Prawo prywatności jako reguła społeczeństwa informacyjnego, red. Chałubińska-Jentkiewicz K., Kakareko K., Sobczak J., Warszawa 2017

Problemy społeczeństwa informacyjnego. Elementy analizy, ewaluacji i prognozy, red. Zacher L., Warszawa 1997

Prywatność a ekonomia. Ochrona danych osobowych w obrocie gospodarczym, red. Mednis A., Warszawa 2013

Prywatność a jawność – bilans 25-lecia i perspektywy na przyszłość, red. Mednis A., wyd. C.H. Beck, Warszawa 2016

Przetwarzanie i ochrona danych, red. Szpor G., Wyd. Stowarzyszenie SILGIS Center, Katowice 1998

Przygotowanie organizacji do stosowania RODO. Ochrona danych w okresie przejściowym i po wejściu przepisów w życie, red. Korga M., wyd. PRESSCOM, Wrocław 2017

Public sector information in the Digit al Age. Between Markets, Public Management and Citizens' Rights, red. Aichholzer G., Burkert H., Cheltenham UK, Northhampton Masachusetts USA, 2004

Reforma ochrony danych osobowych a jawność dostępu do informacji sądowej – aspekty proceduralne, red. Jabłoński M., Flaga-Gieruszyńska K., Wygoda K., Wrocław 2017

RODO. Ogólne rozporządzenie o ochronie danych. Komentarz, red. D. Lubasz, E. Bielak-Jomaa, Warszawa 2017

Robertson R., *Globalization: Social Theory and Global Culture*, Londyn 1992

Rogala-Lewicki A., *Informacja jako autonomiczny czynnik wpływu w przestrzeni publicznej – studium władztwa informacyjnego*, Wydawnictwo Naukowe Grategia, Częstochowa 2016

Rogala-Lewicki A., *Korporacja versus państwo. Arbitraż międzynarodowy z udziałem Polski jako strony postępowania w sporach inwestycyjnych*, Tom I, Kutno 2020

Rogala-Lewicki A., *Korporacja versus państwo. Arbitraż międzynarodowy z udziałem Polski jako strony postępowania w sporach inwestycyjnych. Wybór orzecznictwa sądów arbitrażowych w sprawach z udziałem Polski jako strony sporów inwestycyjnych*, Tom II, Kutno 2020

Rogers E., Kincaid L., *Communication Networks: Towards a New Paradigm for Research*, Nowy Jork 1981

Rojszczak M., *Ochrona prywatności w cyberprzestrzeni z uwzględnieniem zagrożeń wynikających z nowych technik przetwarzania informacji*, Wolters Kluwer, Warszawa 2019

Rosie A.M., *Teoria przesyłania informacji*, przeł. J. Zalewski, Warszawa 1978

Rothert A., *Cybernetyczny porządek polityczny*, Warszawa 2005

Rothert A., *Technopolis, wirtualne sieci polityczne*, Warszawa 2003

Rozporządzenie UE Nr 2015/2120 w zakresie dostępu do otwartego Internetu. Komentarz, red. Piątek S., wyd. 1, Warszawa 2017

Ruszczyk I., *Wzorcowe instrukcje ochrony danych osobowych*, Ośrodek Doradztwa i Doskonalenia Kadr, Gdańsk 1999

Rydlewski G., *Rządzenie w epoce informacji, cyfryzacji i sztucznej* inteligencji, Elipsa Dom Wydawniczy, Warszawa 2021

Rydlewski G., *Rządzenie w świecie megazmian*, Warszawa 2009

Safjan M., *Prawo i medycyna. Ochrona praw jednostki a dylematy współczesnej medycyny*, IWS, Oficyna Naukowa, Warszawa 1998

Sakowska-Baryła M., *Dostęp do informacji publicznej a ochrona danych osobowych, PRESSCOM*, Wrocław 2014

Sakowska-Baryła M., *Orzecznictwo w sprawie udostępniania i odmowy udostępnienia informacji publicznej*, Wyd. I, Municipium S.A, Warszawa 2010

Sakowska-Baryła M., *Prawo do ochrony danych osobowych*, PRESSCOM, Wrocław 2015

Scott J., *Władza*, przeł. S. Królak, Warszawa 2006

Serafin S., Szmulik W., *Organy ochrony prawnej RP*, C.H. Beck, Warszawa 2010

Sfera publiczna. Kondycja, przejawy, przemiany, red. Hudzik J.P., Woźniak W., Lublin 2006

Sibiga G., *Postępowanie w sprawach ochrony danych osobowych*, Dom Wydawniczy ABC, Warszawa 2003

Ochrona danych osobowych. Skuteczność regulacji, red. Szpor G., Warszawa 2009

Stiglitz J., *Globalizacja*, przeł. H. Simbierowicz, Warszawa 2007

Szałowski R., *Prawna ochrona informacji niejawnych i danych osobowych*, Wyd. Difin, Warszawa 2000

Szewc T., *Publicznoprawna ochrona informacji*, C.H. Beck, Warszawa 2007

Szuma K., *Uprawnienia wierzycieli związane z przetwarzaniem w obrocie gospodarczym danych przedsiębiorców – osób fizycznych,* Wydawnictwo Uniwersytetu Ekonomicznego w Poznaniu, Poznań 2013

Tarnacka K., *Prawo do informacji w polskim prawie konstytucyjnym,* Wydawnictwo Sejmowe, Warszawa 2009

The Information Age: An Anthology on Its Impact and Consequences, red. Alberts D.S., Papp D.S., CCRP Publication Series, Waszyngton 1997

The Value and Impact of Information, red. Feeneay M., Grieves M., East Grinstead, West Sussex 1994

Toffler A., *Budowa nowej cywilizacji. Polityka trzeciej fali*, przeł. J. Łoziński, Poznań 1996

Toffler A., *Trzecia fala*, przeł. E. Wojdyłło, Warszawa 1986

Touraine A., *Critique de la modernite*, Fayard, Paryż 1992

Touraine A., *Myśleć inaczej*, przeł. M. Byliniak, Warszawa 2011

Touraine A., *Un nouveau paradigme*, Fayard, Paryż 2005

Tworzenie systemu ochrony danych osobowych krok po kroku, red. Kuc I., wyd. Difin S.A., Warszawa 2016

Unijna reforma ochrony danych osobowych. Analiza zmian, red. Dmochowska A., Zadrożny M., Warszawa 2016

Ustawa o ochronie danych osobowych. Komentarz, red. B. Marcinkowski, Warszawa 2018

Ustawa o ponownym wykorzystywaniu informacji sektora publicznego. Komentarz, red. Piskorz-Ryń A., wyd. PRESSCOM, Wrocław 2016

Vademecum administratora bezpieczeństwa informacji, red. Kołodziej, M., C. H. Beck, Warszawa 2016

Vademecum ABI. Część II – Przygotowanie do roli Inspektora Ochrony Danych, red. Kołodziej M., Warszawa 2017

Wallerstein I., *Koniec świata jaki znamy*, przeł. M. Bilewicz, A.W. Jelonek, K.Tyszka, Warszawa 2004

Wdrażanie systemu ochrony danych osobowych. Praktyczny przewodnik krok po kroku, red. Kuc I., wyd. Difin S.A., Warszawa 2016

Wiewiórowski W., Wierczyński G., *Informatyka prawnicza. Technologia informacyjna dla prawników i administracji publicznej,* Wydawnictwo Zakamycze, Kraków 2006

Wnuk-Lipiński E., *Świat miedzyepoki. Globalizacja. Demokracja. Państwo narodowe*, Kraków 2004

Wociór D., *Ochrona danych osobowych i informacji niejawnych z uwzględnienie ogólnego rozporządzenia unijnego*, Warszawa 2016

Wolność informacji i jej granice, red. Szpor G., Katowice 1998

Wyspecjalizowany organ do spraw dostępu do informacji o charakterze publicznym w wybranych krajach UE, red. Sibiga G., Wyd. I, CH Beck, Warszawa 2013

Zieliński M.Z., *Odpowiedzialność deliktowa pośredniczących dostawców usług internetowych. Analiza prawnoporównawcza*, Wolters Kluwer, Warszawa 2013

Zisk B.H., *The Politics of Transformation: Local Activism in the Peace and Environmental Movements*, Westport 1992

Z problematyki kontroli przetwarzania i ochrony danych osobowych przez Generalnego Inspektora Ochrony Danych Osobowych. Jawność i jej ograniczenia. Zadania i kompetencje, red. Szmulik B., Szpor G., C.H. Beck, Warszawa 2015

Artykuły w drukach zwartych

Banaszak B., *Prawo do ochrony danych osobowych w Polsce* [w:] *O prawach człowieka. W podwójną rocznicę Paktów*, red. Jasudowicz T., Mik C., Księga Pamiątkowa w hołdzie Profesor Annie Michalskiej, Wyd. Dom Organizatora TNOiK, Toruń 1996, s. 249–256

Banyś T., *Wdrażanie nowych elementów systemu ochrony danych osobowych przez podmioty publiczne* [w:] *Polska i europejska reforma ochrony danych osobowych*, red. E. Bielak-Jomaa, D. Lubasz, wyd. Wolters Kluwer, Warszawa 2016, s. 53–62

Czerniawski M., *Portale społecznościowe a prawo do ochrony danych osobowych* [w:] *Internet, Prawno-informatyczne problemy sieci, portali i e-usług*, red. Szpor G., Wiewiórowski W.R., Warszawa 2012 r., s. 163–172

Dmochowska A., *Przetwarzanie danych na podstawie zgody* [w:] *Unijna reforma ochrony danych osobowych. Analiza zmian*, red. A. Dmochowska A., Zadrożny M., Warszawa 2016

Fajgielski P., *Informowanie o naruszeniu ochrony danych osobowych w świetle przepisów ogólnego rozporządzenia o ochronie danych* [w:] *Ogólne rozporządzenie o ochronie danych. Aktualne problemy prawnej ochrony danych osobowych*, red. Sibiga G., Warszawa 2016

Fischer B., *Funkcja kontrolna prasy i jej wykonywanie przez dostęp do informacji publicznej* [w:] *Jawność i jej ograniczenia*, Tom IX. Zadania i kompetencje, red. Szmulik B., wyd. C. H. Beck, Warszawa 2015, s. 346–359

Fischer B., *Instrumenty usuwania sprzeczności między normami prawnymi i technicznymi należącymi do różnych systemów (europejskiego i krajowych)* [w:] *Rejestry publiczne. Jawność i interoperacyjność*, red. Gryszczyńska A., wyd. C. H. Beck, Warszawa 2015, s. 87–107

Fischer B., *Ponadgraniczne przekazywanie danych osobowych – charakter prawny regulacji z uwzględnieniem uzupełniającej roli soft law* [w:] *Prywatność a ekonomia. Ochrona danych osobowych w obrocie gospodarczym*, red. Mednis A., Warszawa 2013, s. 81–90

Fischer B., *Skuteczność ochrony danych osobowych pracowników korporacji z uwzględnieniem ich pozyskania z monitoringu* [w:] *Ochrona danych osobowych. Skuteczność regulacji*, red. Szpor G., Warszawa 2009, s. 167–176

Fischer B. *Wolność wypowiedzi prasowej a prawo do bycia zapomnianym* [w:] *Jawność i jej ograniczenia*, Tom VIII. Postepowania sądowe, red. Gołaczyński J., wyd. C. H. Beck, Warszawa 2015, s. 91–109

Fischer B., *Zasady transferu danych osobowych z Polski na przestrzeni 10 lat obowiązywania ustawy o ochronie danych osobowych* [w:] *10 lat ochrony danych osobowych w Polsce*, red. Fajgielski P., KUL, Lublin 2008, s. 127–140

Hamm R., *Ochrona danych a prawo karne* [w:] O*chrona danych osobowych*, red. Wyrzykowski M., Instytut Spraw Publicznych, Warszawa 1999, s. 73–88

Itrich-Drabarek J., *Jakość i przejrzystość administracji publicznej a prawo dostępu obywateli do informacji* [w:] *Administracje publiczne w Europie – stan obecny i wyzwania przyszłości*, Prace i materiały ISM, SGH, Warszawa 2006, s. 149–161

Kilian W., *Ochrona danych w przedsiębiorstwach* [w:] *Ochrona danych osobowych*, red. Wyrzykowski M., Instytut Spraw Publicznych, Warszawa 1999, s. 99–109

Konarski X., *Ustawa o ochronie danych osobowych a doświadczenia państw Unii Europejskiej* [w:] *Praktyczne konsekwencje obowiązywania ustawy o ochronie danych osobowych*, Seminarium Stowarzyszenia Marketingu Bezpośredniego, Warszawa 1999

Korycka M., *Zasada proporcjonalności – refleksje na gruncie aksjologicznych podstaw Konstytucji z 1997 roku i orzecznictwa Trybunału Konstytucyjnego* [w:] *Wykładnia prawa i inne problemy filozofii prawa*, red. Morawski L., Toruń 2005, s. 43–58

Kotecka S., *Strategie i dobre praktyki dotyczące bezpieczeństwa informacji przetwarzanych w systemach teleinformatycznych i ochrony przed ich nieuprawnionym ujawnieniem* [w:] *Wybrane dobre praktyki w zakresie usług elektronicznych*, red. J. Gołaczyński, Warszawa 2016

Kowalik P., Nowakowski B., *Zastosowanie ustawy o ochronie danych osobowych w jednostkach sektora publicznego* [w:] A. Gałach, S. Hoc, A. Jedruszczak, K. Kędzierska, P. Kowalik, M. Kuźma, R. Marek, B. Nowakowski, *Ochrona danych osobowych i informacje niejawne w sektorze publicznym*, Wydanie 2, Wydawnictwo C.H. Beck, Warszawa 2015

Kowalik P., Wociór D., *Administrator danych w sektorze przedsiębiorstw* [w:] *Ochrona danych osobowych i informacji niejawnych z uwzględnieniem ogólnego rozporządzenia unijnego*, red. Wociór D., Warszawa 2016

Krzysztofek M., *Ochrona danych osobowych w Unii Europejskiej. Transfer danych osobowych z Unii Europejskiej w obecnym i nadchodzącym stanie prawnym* [w:] *Ochrona danych osobowych w Unii Europejskiej*, red. Krzysztofek M., Wolters Kluwer, Warszawa 2014, s. 65–72

Kulesza W., *Ochrona danych osobowych a nowa kodyfikacja prawa karnego w Polsce* [w:] *Ochrona danych osobowych*, red. Wyrzykowski M., Instytut Spraw Publicznych, Warszawa 1999, s. 89–97

Martysz C., *Informacja publiczna czy chronione dane osobowe* [w:] *Ochrona danych osobowych wczoraj, dziś, jutro*, GIODO, Warszawa 2006

Martysz C., *Jawność i jej ograniczenia. Zasady przepływu informacji pomiędzy organami publicznymi* [w:] *Jawność i jej ograniczenia. Zadania i kompetencje*, tom 9, red. Szpor G., Szmulik B., Warszawa 2015

Martysz C., *Prawa osoby w świetle ustawy o ochronie danych osobowych* [w:] *Prawne i finansowe aspekty funkcjonowania samorządu terytorialnego*, Tom 1: Prawo samorządowe i administracyjne, red. Dolaty S., Opole 2000

Martysz C., *Zakres stosowania kodeksu postępowania administracyjnego w ustawie o ochronie danych osobowych* [w:] *Wolność informacji i jej granice*, red. Szpor G., Katowice 1998

Mednis A., *Administrator danych i podmiot przetwarzający dane na zlecenie – status prawny, zakres praw i obowiązków, problemy definicyjne* [w:] *Ochrona danych osobowych – skuteczność regulacji*, red. Szpor G., Municipium SA, Warszawa 2009, str. 78–79

Mednis A., *Dyrektywa 95/46 w świetle orzecznictwa Trybunału Sprawiedliwości Unii Europejskiej – wybrane zagadnienia* [w:] *Prywatność a ekonomia. Ochrona danych osobowych w obrocie gospodarczym*, red. Mednis A., Warszawa 2013, s. 129

Mednis A., *Prywatność od epoki analogowej do cyfrowej – czy potrzebna jest redefinicja?* [w:] *Prywatność a jawność – bilans 25-lecia i perspektywy na przyszłość*, red. Mednis A., wyd. C.H. Beck, Warszawa 2016, s. 1–3

Mednis A., *Transgraniczny przepływ danych osobowych z polskiej perspektywy* [w:] *1998–2013. 15-lecie ustawy o ochronie danych osobowych*, Wydawnictwo Biura Generalnego Inspektora Ochrony Danych Osobowych, Warszawa 2013, s. 40

Mednis A., *Ustawa o ochronie danych osobowych z perspektywy 10-lecia obowiązywania* [w:] *Prawne warunki wymiany informacji – nowe wyzwania*, red. Wierzbowski M. wyd. Stowarzyszenia Absolwentów WPiA UW, s. 153

Mednis A., *Ochrona prywatności i danych osobowych w przepisach prawa pracy – problemy interpretacyjne i konfrontacja z praktyką* [w:] *Ochrona danych podmiotów objętych prawem pracy i prawem ubezpieczeń społecznych*, red. Wyka T., Nerka A., Wolters Kluwer Polska, Warszawa 2012, s. 102–109

Mucha B., *Data mining a współczesny kształt prawa do prywatności w Stanach Zjednoczonych Ameryki* [w:] *Efektywność europejskiego systemu ochrony praw człowieka. Ewolucja i uwarunkowania europejskiego systemu ochrony praw człowieka*, red. Jaskiernia J., Toruń 2012

Rogala-Lewicki A., *Relacje informacyjne państwo – obywatel na tle zależności między e-rządem według Matthew Symondsa, fazami rozwoju demokracji Roberta Alana Dahla, a partycypacją obywatelską* [w:] *Cyberpolitologia. Badanie polityki w Internecie*, red. Mider D., Maksymowicz A., Warszawa 2013

Rogala-Lewicki A., *Informacyjny aspekt decyzji w środowisku politycznym* [w:] *Interdyscyplinarne ujęcie prawa*, red. Żuralska M., Warszawa 2013

Safjan M., *Ochrona danych osobowych – granice autonomii informacyjnej* [w:] *Ochrona danych osobowych*, red. Wyrzykowski M., Instytut Spraw Publicznych, Warszawa 1999, s. 9–17

Sakowska-Baryła M., *Ograniczenia prawa do ponownego wykorzystywania ISP* [w:] *Ponowne wykorzystywanie informacji sektora publicznego*, red. Sibiga G., Ministerstwo Cyfryzacji, Warszawa 2016, s. 54–105.

Sakowska-Baryła M., *Organizacja ochrony danych osobowych w ramach wspólnej obsługi w centrum usług wspólnych* [w:] *Samorządowe centra usług wspólnych,* red. Sakowska-Baryła M., Górski M., wyd. MUNICIPIUM, Warszawa 2017, s. 177–197

Sakowska-Baryła M., *Problem współstosowania ustawy o dostępie do informacji publiczne i ustawy o ochronie danych* osobowych [w:] *Prywatność a jawność – bilans 25-lecia i perspektywy na przyszłość*, red. Mednis A., C.H. Beck, Warszawa 2016, s. 173–192

Sakowska-Baryła M., *Prywatność w inteligentnym mieście* [w:] *Internet rzeczy. Bezpieczeństwo w Smart city*, red. Szpor G., C.H. Beck, Warszawa 2015, s. 129–144

Sakowska-Baryła M., *System informacji oświatowej* [w:] *Internet. Prawno-informatyczne problemy sieci, portali i e-usług,* red. Szpor G., Wiewiórowski W., CH Beck, Warszawa 2012, str. 315–323

Sakowska-Baryła M., *Udostępnianie danych osobowych na gruncie ustawy o ochronie danych osobowych* [w:] *Ochrona danych osobowych w Polsce z perspektywy dziesięciolecia*, red. Fajgielski P., Wydawnictwo KUL, Lublin 2008, s. 103–126

Sibiga G., *Administrator bezpieczeństwa informacji (uwagi de lege lata)* [w:] *Ochrona informacji niejawnych, biznesowych i danych osobowych*, red. Gajos M., Krajowe Stowarzyszenie Ochrony Informacji Niejawnych i Uniwersytet Śląski, Katowice 2010, s. 165–172

Tinnefeld M.Th., *Ochrona danych – kamień węgielny budowy Europy* [w:] *Ochrona danych osobowych*, red. Wyrzykowski M., Instytut Spraw Publicznych, Warszawa 1999, s. 33–48

Wyrzykowski M., *Ochrona danych – zagadnienia konstytucyjne* [w:] *Ochrona danych osobowych*, red. Wyrzykowski M., Instytut Spraw Publicznych, Warszawa 1999, s. 19–32

Zadrożny M., *Warunki nakładania przez GIODO administracyjnych kar pieniężnych* [w:] *Unijna reforma ochrony danych osobowych. Analiza zmian*, red. Dmochowska A., Zadrożny M., Warszawa 2016

Artykuły

Barta J., Markiewicz R., *Świadczenie usług drogą elektroniczną – nowa rzeczywistość dla prawników*, Radca Prawny 2002, nr 4–5

Bielak-Jomaa E., *Wyzwania przed administratorami bezpieczeństwa informacji (inspektorami ochrony danych) w związku z wejściem w życie ogólnego rozporządzenia o ochronie danych*, Monitor prawniczy 2016, nr 20

Bienias M., *Ochrona danych w fazie projektowania oraz domyślna ochrona danych (privacy by design oraz privacy by default) w ogólnym rozporządzeniu o ochronie danych*, Monitor prawniczy 2016, nr 20

Bierć A., *Sytuacja prawna administratora bezpieczeństwa informacji, jako podmiotu zobowiązanego do kontroli stanu ochrony danych osobowych w przedsiębiorstwie*, Przegląd Legislacyjny 2000, nr 4

Borecka J., *Geneza prawnej ochrony danych osobowych i pojęcie danych osobowych*, Zeszyty Naukowe Instytutu Administracji Akademii im. Jana Długosza w Częstochowie 2006, nr 4

Boruta I., *Ochrona dóbr osobistych pracownika*, Praca i Zabezpieczenie Społeczne 1998, nr 2

Byczkowski M., *Lista kontrolna ABI*, Biuletyn Administratorów Bezpieczeństwa Informacji: Ochrona Danych Osobowych 2000, nr 2

Byczkowski M., *Przygotowanie ABI do nowej funkcji inspektora ochrony danych*, Informacja w administracji publicznej 2017, nr 1

Byczkowski M., *Zabezpieczanie danych osobowych w RODO*, Informacja w administracji publicznej 2017, nr 2

Byrski J., Hoser H., *Social media oraz technologie umożliwiające śledzenie użytkowników Internetu a współadministrowanie danymi osobowymi*, Monitor Prawniczy – dodatek specjalny, Prawo nowych technologii 2019, nr 21

Byrski J., *Umowne powierzenie do przetwarzania danych osobowych w ustawie o ochronie danych osobowych, dyrektywie 95/46 i w ogólnym rozporządzeniu o ochronie danych*, Monitor prawniczy 2016, nr 20

Chołodecki M., *Model kontroli sądowej decyzji Prezesa Urzędu Komunikacji Elektronicznej*, Internetowy Kwartalnik Antymonopolowy i Regulacyjny 2012, nr 6 (1)

Ciechomska M., *Zmiana Konwencji nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych szansą na powstanie globalnego instrumentu ochrony danych*, Monitor prawniczy 2017, nr 16

Czerniawski M., *Aktualny i projektowany zakres terytorialny unijnych przepisów o ochronie danych osobowych,* Europejski Przegląd Sądowy 2015, nr 5

Drozd A., *Uprawnienie podmiotu zatrudniającego do pozyskiwania informacji o kandydacie na pracownika*, Państwo i Prawo 2000, nr 12

Fajgielski P., *Administrator bezpieczeństwa informacji – geneza, stan obecny i perspektywa zmian*, Monitor Prawniczy z 2014, nr 9

Fajgielski P., *Informowanie o naruszeniu ochrony danych osobowych w świetle przepisów ogólnego rozporządzenia o ochronie danych*, Monitor Prawniczy 2016, nr 20

Fajgielski P., *Obowiązek informacyjny w ogólnym rozporządzeniu o ochronie danych*, Informacja w administracji publicznej 2017, nr 1

Fajgielski P., *Przetwarzanie szczególnych kategorii danych w świetle RODO*, Informacja w administracji publicznej 2017, nr 2

Fajgielski P., *Zgoda na przetwarzanie danych osobowych w przepisach ogólnego rozporządzenia o ochronie danych*, Informacja w administracji publicznej 2017, nr 4

Fischer B., *Administrator danych osobowych po przystąpieniu Polski do Unii Europejskiej. Uwagi de lege lata*, Radca Prawny z 2004, nr 5

Fischer B., Karwala D., *Umowy transferowe jako instrument przekazywania danych osobowych do państw trzecich*, Przegląd Prawa Handlowego 2007, nr 10

Fischer B., *Przestępstwa komputerowe i ochrona informacji*, Państwo i Prawo 2001, nr 1

Fischer B., *Wiążące reguły i wzajemne uznawanie w nowelizacji OchrDanOsobU z 2015 r. oraz wspieranie efektywnego funkcjonowania tego instrumentu,* Monitor Prawniczy 2015, nr 6

Fischer B., *Wybrane problemy prawne przekazywania danych osobowych do państw trzecich w praktyce korporacyjnej*, Przegląd Corporate Governance 2007, nr 3

Giermak M., Sofronów M., *Zgoda na przetwarzanie danych osobowych dzieci w serwisach społecznościowych w kontekście zmian prawa europejskiego*, Monitor prawniczy 2017, nr 2

Goik Z., *Forma udostępnienia (odmowy udostępnienia) danych osobowych*, Radca Prawny 2000, nr 1

Góral Z., *Odpowiedzialność porządkowa w świetle najnowszego orzecznictwa sądowego*, Praca i Zabezpieczenie Społeczne 2002, nr 11

Grzegory T., *Pamięć absolutna czy kontrolowana amnezja – wybrane problemy prawne regulacji „prawa do bycia zapomnianym" w ogólnym rozporządzeniu o ochronie danych*, Monitor prawniczy 2016, nr 20

Hoc S., *Problem stosowania wobec sędziów ustawy o ochronie informacji niejawnych*, Państwo i Prawo 2000, nr 5

Itrich-Drabarek J., *Prawo dostępu do informacji o działalności administracji publicznej w* państwach *demokratycznych*, Świat i Polityka 2002, nr 1/2

Iwaszko B., *Bezpieczeństwo akredytowane*, IT w Administracji 2012, nr 8

Iwaszko B., *Bezpieczeństwo systemów teleinformatycznych*, IT w Administracji 2012, nr 12

Iwaszko B., *Bezpieczeństwo szczególnie wymagane*, IT w Administracji 2012, nr 9

Jackowiak U., *Ochrona danych osobowych w prawie pracy,* Praca i Zabezpieczenie Społeczne 1998, nr 3

Jachimowicz M., *Przestępstwo zakłócenia kontroli (art. 225 k.k.)*, Prokuratura i Prawo 2008, nr 7–8

Kalinowska N., Litwiński P., *Ocena skutków dla ochrony danych i uprzednie konsultacje – nowe obowiązki podmiotów przetwarzających dane osobowe*, Monitor prawniczy 2017, nr 13

Kamiński M., *Uwięzione dane osobowe*, IT w Administracji 2012, nr 11

Kawecki M., Kozieł K., *Ochrona wizerunku w systemie ochrony danych osobowych,* Internetowy Przegląd Prawniczy TBSP UJ 2012, nr 3

Kędzierska K., *Umowa o pracę z administratorem bezpieczeństwa informacji*, Informacja w administracji publicznej 2017, nr 4

Kluska M., *Dane chronione na nowo*, IT w Administracji 2012, nr 6

Knapp V., *Rozważania nad możliwością stosowania cybernetyki w dziedzinie prawa*, Państwo i Prawo 1996, nr 4

Konarski X., *Profilowanie danych osobowych na podstawie ogólnego rozporządzenia o ochronie danych osobowych – dotychczasowy i przyszły stan prawny w UE*, Monitor prawniczy 2016, nr 20

Konarski X., Sibiga G., *Zmiany w ustawie o ochronie danych osobowych w świetle Dyrektywy 95/46/WE*, Monitor Prawniczy 2004, nr 12

Kordasiewicz B., *Cywilnoprawna ochrona prawa do prywatności*, Kwartalnik Prawa Prywatnego 2000, nr 1

Korga M., *Dane biometryczne i ich wykorzystywanie na gruncie stosunku pracy*, Monitor Prawa Pracy 2011, nr 12

Korga M., *Przetwarzanie danych biometrycznych pracowników w świetle orzeczenia NSA z dnia 1 grudnia 2009r.*, Studia Prawnicze 2011, nr 1 (187)

Kowalczuk-Pakuła I., Chołuj M., *Współadministrowanie – nowy paradygmat w prawie ochrony danych osobowych*, Monitor Prawniczy – dodatek specjalny, Prawo nowych technologii 2019, nr 21

Krzysztofek M., *Ochrona danych w fazie projektowania i domyślna ochrona danych*, Informacja w administracji publicznej 2017, nr 1

Krzysztofek M., *Prawo do bycia zapomnianym i inne aspekty prywatności w epoce Internetu w prawie UE*, Europejski Przegląd Sądowy 2012, nr 8

Krzysztofek M., *Przekazywanie z UE do USA danych z komunikatów finansowych w systemie SWIFT*, Państwo i Prawo 2011, nr 7–8

Krzysztofek M., *Sprawdzenie gotowości instytucji do wdrożenia reformy ochrony danych osobowych*, Informacja w administracji publicznej 2017, nr 4

Kuczyński T., *Ochrona danych osobowych w stosunkach zatrudnienia*, Przegląd Sądowy 1998, nr 11/12

Kuisz J., *Konstytucja w sytuacjach zagrożenia bezpieczeństwa państwa na tle teorii R.A. Posnera*, Państwo i Prawo 2013, nr 12

Kulesza E., *Ochrona danych o stanie zdrowia w świetle ustawodawstwa europejskiego i polskiej ustawy o ochronie danych osobowych*, Prawo i Medycyna 2000, nr 5

Kulesza E., *Pozycja i uprawnienia Generalnego Inspektora Ochrony Danych Osobowych w świetle Ustawy o ochronie danych osobowych. Uwagi de lege lata i de lege ferenda*, Przegląd Sejmowy 1999, nr 6 (35)

Kuner C., *Reality and Illusion in EU Data Transfer Regulation Post Schrems*, University of Cambridge Faculty of Law Research Paper 2016, nr 14

Kurzępa B., *Przestępstwa z ustawy o ochronie danych osobowych*, Prokuratura i Prawo 1999, nr 6

Leja P., *Ochrona danych osobowych a Internet rzeczy, profilowanie i repersonalizacja danych*, Prawo Mediów Elektronicznych 2017, nr 3

Levin A., Nicholson M., *Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground*, University of Ottawa Law & Technology Journal 2005, nr 2

Litwiński P., *Monitoring pracownika w miejscu pracy a ochrona danych osobowych pracownika*, Monitor Prawa Pracy 2008, nr 2

Litwiński P., *Pojęcie danych osobowych w rozporządzeniu ogólnym o ochronie danych osobowych*, Informacja w administracji publicznej 2017, nr 3

Litwiński P., *Udostępnianie danych osobowych na potrzeby postępowań cywilnych*, Przegląd Prawa Technologii Informacyjnych. ICT Law Review 2013, nr 1

Litwiński P., *Udostępnianie danych osobowych przez organy administracji samorządowej*, Państwo i Prawo 2006, nr. 1

Lubasz D., *Przekazywanie danych osobowych do państw trzecich w ogólnym rozporządzeniu o ochronie danych*, Monitor prawniczy 2016, nr 20

Mattioli M., *Disclosing Big Data*, Minnesota Law Review 2014, nr 99

Mazur M., *Publiczne dane osobowe,* IT w Administracji 2012, nr 2

Mednis A., *Administracyjne kary pieniężne w ogólnym rozporządzeniu i ochronie danych*, Informacja w administracji publicznej 2017, nr 3

Mednis A., *Obowiązki podmiotów prywatnych wykorzystujących dane osobowe*, Monitor Prawniczy 1998, nr 8, s. 293–296

Mednis A., *Ochrona danych na temat stanu zdrowia*, Biuletyn Ochrony Danych Osobowych 2000, nr 8

Mednis A., *Ochrona danych osobowych i ochrona prywatności w świetle dyrektywy UE z dnia 12 lipca 2002 roku o prywatności w komunikacji elektronicznej*, Prawo i Ekonomia w Telekomunikacji 2002, nr 4

Mednis A., *Ochrona danych osobowych w Konwencji Rady Europy i Dyrektywie Unii Europejskiej*, Państwo i Prawo 1996, nr 6

Mednis A., *Ochrona danych osobowych w Konwencji Rady Europy i Dyrektywie Unii Europejskiej cz. I*, Biuletyn Administratorów Bezpieczeństwa Informacji: Ochrona Danych Osobowych 2000, nr 1

Mednis A., *Ochrona danych osobowych w Konwencji Rady Europy i Dyrektywie Unii Europejskiej cz. II*, Biuletyn Administratorów Bezpieczeństwa Informacji: Ochrona Danych Osobowych 2000, nr 2

Mednis A., *Państwo wobec praw jednostki (na tle orzecznictwa Europejskiej Komisji i Europejskiego Trybunału Praw Człowieka do art. 8 Europejskiej Konwencji Praw Człowieka)*, Samorząd Terytorialny 2000, nr 12 (40)

Mednis A., *Postulowane zmiany w ustawie o ochronie danych osobowych*, Biuletyn Administratorów Bezpieczeństwa Informacji: Ochrona Danych Osobowych 2000, nr 3

Mednis A., *Reforma europejskich regulacji prawnych dotyczących ochrony danych osobowych – najważniejsze kierunki proponowanych zmian*, Informacja w administracji publicznej 2015, nr 1

Mednis A., Rudzińska K., *Przetwarzanie danych osobowych podczas postępowania kontrolnego prowadzonego przez Najwyższą Izbę Kontroli*, Przegląd Metodyczny 2012, nr 3

Mednis A., *Udostępnianie danych o stanie zdrowia*, Biuletyn Ochrony Danych Osobowych 2000, nr 9

Mednis A., *Ustawa o ochronie danych osobowych – wprowadzenie,* Biuletyn Ochrony Danych Osobowych 2000, nr. 1

Mednis A., *Uwagi do projektu ustawy o zmianie ustawy o ochronie danych osobowych*, Biuletyn Ochrony Danych Osobowych 2001, nr 17

Mednis A., *Wymóg oceny skutków przetwarzania w ogólnym rozporządzeniu o ochronie danych*, Monitor prawniczy 2016, nr 20

Michałowicz A., *Nowe zasady transferu danych osobowych z Unii Europejskiej do Stanów Zjednoczonych w ramach tarczy Prywatności*, Monitor prawniczy 2016, nr 23

Morawski F., *Odpowiedzialność cywilna administratora danych osobowych i podmiotu przetwarzającego według ogólnego rozporządzenia o ochronie danych osobowych*, Acta Iuris Stetinensis 2019, Nr 26

Mucha M., *Ograniczenia zasady jawności i dostępu do informacji – regulacje administracyjnoprawne*, Samorząd Terytorialny 2000, nr 1/2

Mystek K., *Sprawdzanie dokonywane przez ABI na zlecenie GIODO*, Ekspert Ochrony Informacji 2016, nr 1 (7)

Mystek K., Zgoda *na przetwarzanie danych osobowych dla realizacji wniosku. Uwagi krytyczne*, Ekspert Ochrony Informacji 2016, nr 3 (9)

Nowelizacja ustawy o ochronie danych osobowych 2010, red. Sibiga G., MoP dodatek specjalny 2011, nr 3

Nowicki M.A., *Ile informacji, ile prywatności,* Prawo i Życie 2000, nr 10

Oleksiuk I., *Prawo do prywatności w Internecie. Wybrane rozwiązania prawne USA i Kanady*, Przegląd Ustawodawstwa Gospodarczego 2000, nr 3

Osiej T., *Charakter prawny nowych mechanizmów certyfikacji w zakresie ochrony danych osobowych*, Informacja w administracji publicznej 2017, nr 2

Piech M., *One stop shop. Mechanizmy podejmowania decyzji w sprawie transgranicznego przetwarzania danych osobowych w UE*, Monitor prawniczy 2016, nr 20

Rogala-Lewicki A., *Citizens' involvement in public sphere – information as a ius publicum factor of the state of democracy,* European Journal of Geopolitics, Nr 5/2017

Rogala-Lewicki, A., *Classified methods of collecting information on citizens. Comparative legal study of invigilation in Poland*, Studium Europy Środkowej i Wschodniej, Nr 14/2020

Rogala-Lewicki A., *Dane osobowe w systemach informacyjnych Schengen (SIS, VIS) – ochrona i nadzór instytucjonalny*, Wiedza Prawnicza, Nr 5/2013

Rogala-Lewicki A., *Dane osobowe – zagrożenia wynikające z aktywności sektora państwowego w przestrzeni niejawnej*, Wiedza Prawnicza Nr 6/2013

Rogala-Lewicki A., *Dane osobowe w systemach państwowych – uprawnienia podmiotowe i sankcje*, Wiedza Prawnicza, Nr 1/2014

Rogala-Lewicki A., *European Intelligence Community – the unfulfilled pillar of the European Union*, Myśl Ekonomiczna i Polityczna, Nr 3(54)/2016

Rogala-Lewicki A., *Ład światowy w ujęciu kosmopolitycznym – studium koncepcji Davida Helda*, Przegląd Geopolityczny, Nr 7/2014

Rogala-Lewicki A., *Norwegia versus Unia Europejska – uprzywilejowane partnerstwo, integracja outsidera, czy selektywna współpraca*, Myśl Ekonomiczna i Polityczna, Nr 1(52)/2016

Rogala-Lewicki, A., *Participation of intelligence services in political decision-making proces – evolution of coorditation patterns in Poland*, Studium Europy Środkowej i Wschodniej, Nr 13/2020

Rogala-Lewicki A., *Security services after the terrorist attacks in the US and Europe. Patriot Act versus the Retention Directive, or the legitimization of abuses in the sphere of privacy in democratic states: a comparative study*, Myśl Ekonomiczna i Polityczna, Nr 3(50)/2015

Rogala-Lewicki A., *Struktura organizacyjna służb specjalnych – ilustracja w oparciu o wybrane modele państw i systemy polityczne*, Studium Europy Środkowej i Wschodniej, Nr 6/2016

Rogala-Lewicki A., *Systemy wspierające decyzje w procesie zarządzania politycznego*, Studium Europy Środkowej i Wschodniej, Nr 4/2015

Rogala-Lewicki A., *Transparency and public information policy in Norway – a model to follow for Central-Eastern European states*, Studium Europy Środkowej i Wschodniej, Nr 3/2015

Rogala-Lewicki A., *Usytuowanie funkcjonalne służb specjalnych w systemie politycznym państwa na przykładzie Polski*, Studium Europy Środkowej i Wschodniej, Nr 5/2016

Rojszczak M., *Analiza i praktyczne uwagi w zakresie konstrukcji i stosowania prawa do bycia zapomnianym w UE*, Prawo Mediów Elektronicznych 2017, nr 3

Rojszczak M., *Prawne podstawy prowadzenia masowej inwigilacji obywateli opartej na hurtowym i nieukierunkowanym przechwytywaniu danych w UE z uwzględnieniem dorobku orzeczniczego TSUE i ETPC*, Studia Prawa Publicznego 2017, nr 2,

Rojszczak M., *Skuteczność ochrony praw podmiotów danych wynikających z prawa UE w świetle umowy Tarcza Prywatności oraz prawodawstwa federalnego USA*, Transformacje Prawa Prywatnego 2018, nr 1

Rokita K., *Niezależność organów ochrony danych osobowych w ogólnym rozporządzeniu o ochronie danych*, Europejski Przegląd Sądowy 2016, nr 7

Rubinstein I., *Big Data: The End of Privacy or a New Beginning?*, International Data Privacy Law 2013, nr 2

Safjan M., *Prawo do prywatności i ochrona danych osobowych w społeczeństwie informatycznym*, Państwo i Prawo 2002, nr 6

Sakowska-Baryła M., *ABI i IOD w placówce oświatowej*, TIK w edukacji 2016, nr 5

Sakowska-Baryła M., *Dostęp do informacji o osobach pełniących funkcje publicznej w świetle orzecznictwa i praktyki*, Informacja w Administracji Publicznej 2016, nr 2

Sakowska-Baryła M., *Konstytucjonalizacja prawa do ochrony danych osobowych*, Przegląd Prawa Konstytucyjnego 2016, nr 4

Sakowska-Baryła M., *Kontrolowanie przez GIODO przetwarzania danych osobowych*, Kontrola Państwowa 2016, nr 2

Sakowska-Baryła M., *Obowiązek wyznaczenia IOD w podmiotach publicznych*, ABI Expert 2017, nr 2

Sakowska-Baryła M., *Podmiotowy zakres ustawy o ochronie danych osobowych*, Radca Prawny 2006, nr 6

Sakowska-Baryła M., *Pojęcie „zbiór danych" na gruncie ustawy o ochronie danych osobowych*, Radca Prawny 2005, nr 2

Sakowska-Baryła M., *Pozycja ustrojowa i zadania Generalnego Inspektora Ochrony Danych Osobowych*, Przegląd Sejmowy 2006, nr 2

Sakowska-Baryła M., *Udostępnianie informacji o osobach pełniących funkcje publiczne w praktyce samorządu terytorialnego*, Przedsiębiorczość i Zarządzanie 2017, nr 2

Sakowska-Baryła M., *Współstosowanie ustaw o dostępie do informacji publicznej i ochronie danych osobowych przy udostępnianiu informacji o osobie pełniącej punkcję publiczną*, Orzecznictwo Sądu Apelacyjnego w Łodzi 2015, nr 2

Sibiga G., *Dopuszczalny zakres polskich przepisów o ochronie danych osobowych po rozpoczęciu obowiązywania ogólnego rozporządzenia o ochronie danych – wybrane zagadnienia*, Monitor prawniczy 2016, nr 20

Sibiga G., *Ochrona danych osobowych: zmiany w prawie w latach 2010–2012 oraz planowana reforma systemu*, Edukacja Prawnicza 2012, nr 10

Sibiga G., *Ogólne rozporządzenie o ochronie danych. Aktualne problemy prawnej ochrony danych osobowych 2016 – Wprowadzenie*, Monitor prawniczy 2016, nr 20

Sibiga G., *Przetwarzanie i ochrona danych osoby ubiegającej się o zatrudnienie w świetle przepisów prawa pracy*, Radca Prawny 2005, nr 2

Sibiga G., *Zakres stosowania ustawy o ochronie danych osobowych do przetwarzania danych osobowych pracowników i osób ubiegających się o zatrudnienie*, Monitor Prawa Pracy 2012, nr 3

Sibiga G., *Zgłoszenie zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych*, Monitor Prawniczy 1999, nr 8

Siostrzonek A., *Dane osobowe gromadzone w bazach danych i ich ochrona w prawie polskim*, Rejent 1999 r, nr 9

Siwicki M., *Ochrona danych osobowych w zatrudnieniu w chmurze obliczeniowej*, Monitor prawniczy 2016, nr 20

Siwicki M., *Ochrona osób fizycznych w związku z przetwarzaniem i swobodnym przepływem danych osobowych*, Państwo i Prawo 2016, nr 3

Sobczak J., *Dane osobowe przetwarzane w chmurze obliczeniowej*, Informacja w administracji publicznej 2017, nr 2

Sut P., *Problem twórczej wykładni przepisów o ochronie dóbr osobistych*, Państwo i Prawo 1997, nr 9

Syska K., *Administrator bezpieczeństwa informacji a inspektor ochrony danych – porównanie przesłanek powołania, statusu i zadań*, Monitor prawniczy 2016, nr 20

Szczotkowska M., *Regulacje prawne transferu danych osobowych obywateli UE do USA – prawnoporównawcza analiza programu Safe Harbour i programu Privacy Shield*, Folia Iuridica Universitatis Wratislaviensis 2016, nr. 5 (1)

Szewc T., *Udostępnianie danych osobowych na wniosek*, Monitor Prawniczy 2006, nr 22

Szpor G., *Publicznoprawna ochrona danych osobowych*, PUG 1999, nr 12

Szymielewicz K., *Reforma europejskiego prawa o ochronie danych osobowych z perspektywy praw obywateli – więcej czy mniej ochrony?*, Monitor prawniczy 2016, nr 20

Szymielewicz K., Walkowiak A., *Autonomia informacyjna w kontekście usług internetowych: o znaczeniu zgody na przetwarzanie danych i ryzykach związanych z profilowaniem*, Monitor Prawniczy 2014, nr 9

Taras W., *Pojęcie „informacja" jako narzędzie badania administracji publicznej*, Samorząd Terytorialny 2000, nr 12

Wiewiórowski W.R., *Prywatność pacjenta musi być chroniona*, IT w Administracji 2013, nr 2

Wolska-Bagińska A., *Podstawy prawne przetwarzania danych osobowych w postępowaniu karnym*, Prokuratura i Prawo 2018, nr 6

Wygoda K., *Polska Ustawa o ochronie danych osobowych jako jedna z gwarancji prawa do prywatności*, Humanistyczne Zeszyty Naukowe „Prawa Człowieka" 1998, nr 5

Zalewska-Wojtuś K., *Dyrektywa jako źródło prawa*, Energia Elektryczna 2010, nr 2

Zimna M., *Odpowiedzialność karna za naruszenie ochrony danych osobowych*, Prokuratura i Prawo 2020, nr 1

Zimny W., *Czy adresy e-mailowe są danymi osobowymi?*, Biuletyn Ochrony Informacji 2002, nr 2

Zimny W., *Legalność ustanowienia, relacja do Administratora danych i rola Administratora bezpieczeństwa informacji*, Biuletyn Administratorów Bezpieczeństwa Informacji: Ochrona Danych Osobowych 2000, nr 1

Zimny W., *Ocena podstawowych obowiązków zarządu spółki prowadzącej zarejestrowany zbiór danych osobowych w świetle ustawy o ochronie danych osobowych*, ODO 2001, nr 23

Zimny W., *Omówienie przedłożenia rządowego nowelizacji ustawy o ochronie danych osobowych*, ODO 2001, nr 17

Zimny W., *Praktyczne skutki nowelizacji ustawy o ochronie danych osobowych z dnia 25 sierpnia 2001 r.*, ODO 2001, nr 21

Zimny W., *Udostępnianie danych osobowych w trybie art. 29 ustawy o ochronie danych osobowych*, ODO 2000, nr 7

Zimny W., *Umowa powierzenia przetwarzania danych oraz rola administratora bezpieczeństwa informacji w procesie zawierania i realizacji tej umowy*, ODO 2001, nr 18/19

Zoll A., *Ochrona prywatności w prawie karnym*, Czasopismo Prawa Karnego 2000, nr 1

Źródła internetowe

7 principles of Privacy by Design, https://dataprivacymanager.net/seve-principles-of-privacy-by-design-and-default-what-is-data-protection-by-design-and-default/, [dostęp: 17.12.2020]

50 mln euro kary dla Google za naruszenie RODO, https://niebezpiecznik.pl/post/50-mln-euro-kary-dla-google-za-naruszenie-rodo/, [dostęp: 30.12.2020]

ABC zabezpieczania danych osobowych – środki techniczne i organizacyjne, https://cognitio.edu.pl/abc-zabezpieczania-danych-osobowych-srodki-techniczne-i-organizacyjne/, [dostęp: 10.12.2020]

ABC zasad kontroli przetwarzania danych osobowych, Biuro Generalnego Inspektora Danych Osobowych, Warszawa 2011, s. 6, file:///C:/Users/adwokat/Downloads/ABC-zasad-kontroli-przetwarzania-danych-osobowych.pdf, [dostęp: 25.11.2020]

Adequuacy decisions. How the EU determines if a non-EU country has an adequate level of data protection, European Commission, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en#relatedlinks, [dostęp: 07.12.2020]

Anonimizacja i pseudonimizacja danych – techniki ochrony danych, Newsletter UODO dla Inspektorów Ochrony Danych 2021, nr 4 (25), https://rodoprotektor.pl/anonimizacja-i-pseudonimizacja-danych-osobowych/, [dostęp: 17.12.2020]

Apple ma zapłacić 1,2 mld USD kary za praktyki antykonkurencyjne, https://ithardware.pl/aktualnosci/apple_ma_zaplacic_1_2_mld_usd_kary_za_praktyki_antykonkurencyjne-11716.html, [dostęp: 30.07.2021]

Apple oskarżone przez EU, grozi im kara w wysokości 27 mld USD, https://antyweb.pl/apple-oskarzone-przez-eu-grozi-im-kara-w-wysokosci-27-mld-usd, [dostęp: 30.07.2021]

Artykuł 7 – Warunki wyrażenia zgody, https://gdpr.pl/baza-wiedzy/akty-prawne/interaktywny-tekst-gdpr/artykul-7-warunki-wyrazenia-zgody, [dostęp: 15.11.2020]

Artykuł 35 – Ocena skutków dla ochrony danych, GDPR.PL, https://gdpr.pl/baza-wiedzy/akty-prawne/interaktywny-tekst-gdpr/artykul-35-ocena-skutkow-dla-ochrony-danych, [dostęp: 13.12.2020]

Balcerzak T., *Bezpieczny lot, bezpieczne dane*, http://www.europedirect.um.warszawa.pl/aktualnosci/bezpieczny-lot-bezpieczne-dane, [dostęp: 5.10.2021]

Bała A., *Holandia: Zbieranie danych przez Windows 10 nielegalne*, https://www.purepc.pl/holandia-zbieranie-danych-przez-windows-10-nielegalne, [dostęp: 30.12.2020]

Bernatek G., *Pseudonimizacja danych*, https://rodoradar.pl/pseudonimizacja-danych/, [dostęp: 19.12.2020]

Bęza M., Kolejna kara za naruszenie przepisów RODO, https://home.kpmg/pl/pl/home/insights/2019/10/rodonews-kolejna-kara-za-naruszenie-przepisow-rodo.html, [dostęp: 30.12.2020]

Bieńkowski M., *7 grzechów projektowania sieci Wi-Fi*, https://www.computerworld.pl/news/7-grzechow-projektowania-sieci-Wi-Fi,413368.html, [dostęp: 19.12.2020]

Bodzak K., *Nowe standardowe klauzule umowne Komisji Europejskiej*, https://rodoradar.pl/nowe-standardowe-klauzule-umowne-komisji-europejskiej/, [dostęp: 07.07.2021]

Borowska A., *Powierzenie danych osobowych – na czym polega?*, https://poradnikprzedsiebiorcy.pl/-na-czym-polega-powierzenie-danych-osobowych, [dostęp: 15.12.2020]

Buczkowski K., *Prawnokarna problematyka ochrony danych osobowych*, Warszawa 2015, s. 3, https://iws.gov.pl/wp-content/uploads/2018/08/IWS_Buczkowski-K._Prawnokarna-problematyka-ochrony-danych-osobowych.pdf, [dostęp: 07.12.2020]

Certyfikat zgodności z RODO, https://lexdigital.pl/certyfikat-zgodnosci-z-rodo, [dostęp: 18.08.2021]

Chodorowski M., *Największe wyzwanie RODO – on risk based approach*, https://s4edu.pl/pl/centrum-wiedzy/92-gdpr/116-najwieksze-wyzwanie-rodo-on-riks-based-approach, [dostęp: 30.05.2020]

Czym jest Europejska Rada Ochrony Danych Osobowych i jakie ma zadania?, https://www.politykabezpieczenstwa.pl/pl/a/czym-jest-europejska-rada-ochrony-danych-osobowych-i-jakie-ma-zadania, [dostęp: 01.07.2021]

Czym są standardowe klauzule umowne przyjęte przez KE?, https://blog-daneosobowe.pl/czym-sa-standardowe-klauzule-umowne-przyjete-przez-ke-rodofaq/, [dostęp: 07.07.2021]

Decyzja 2001/479/WE Komisji z 15.06.2001 r. w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich, http://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32001D0497&from=en, [dostęp: 10.12.2021]

Decyzja 2004/915/WE Komisji z 27.12.2004 r. zmieniająca decyzję 2001/497/WE w zakresie wprowadzenia alternatywnego zestawu standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:385:0074:0084:PL:PDF, [dostęp: 10.12.2021]

Decyzja 2010/87/UE Komisji z 05.02.2010 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, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:PL:PDF, [dostęp: 10.12.2021]

Dela M., *Rejestracja zbioru danych osobowych*, Kwartalnik Naukowy Prawo Mediów Elektronicznych 2010, nr 2, http://www.bibliotekacyfrowa.pl/Content/38667/PDF/010.pdf, [dostęp: 19.10.2020]

DK SA Standard Contractual Clauses for the purposes of compliance with art. 28 GDPR (January 2020), European Data Protection Board, https://edpb.europa.eu/our-work-tools/our-documents/decision-sa/dk-sa-standard-contractual-clauses-purposes-compliance-art_en, [dostęp: 07.07.2021]

Druś M., *Amazon.com ukarany 746 mln EUR za naruszenie RODO*, https://www.pb.pl/amazon-com-ukarany-746-mln-eur-za-naruszenie-rodo-1123493, [dostęp: 30.07.2021]

EDPB-EDPS Joint Opinion 1/2021 on standard contractual clauses between controllers and processors, European Data Protection Board, https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-12021-standard_en, [dostęp: 07.07.2021]

EDPB-EDPS Joint Opinion 2/2021 on standard contractual clauses for the transfer of personal data to third countries, European Data Protection Board, https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-22021-standard_en, [dostęp: 07.07.2021]

EDPB Releases Guidance for EU-US Data Transfers, https://digit.fyi/edpb-releases-guidance-for-eu-us-data-transfers/, [dostęp: 10.12.2020]

Europejski Obszar Gospodarczy (EOG), Szwajcaria i kraje północy, Parlament Europejski https://www.europarl.europa.eu/ftu/pdf/pl/FTU_5.5.3.pdf, [dostęp:17.12.2020]

Facebook zapłaci karę za aferę Cambridge Analytica, https://businessinsider.com.pl/wiadomosci/kara-dla-facebooka-za-afere-cambridge-analytica/9e6yzdd, [dostęp: 30.12.2020]

Gerunov A., *Privacy by Design in Practice,* https://logsentinel.com/blog/privacy-by-design-in-practice/, [dostęp: 17.12.2020]

GIODO: ustawa 500 plus próbuje zmodyfikować podstawowe zasady przetwarzania danych osobowych, https://samorzad.infor.pl/sektor/zadania/opieka_spoleczna/737744,GIODO-ustawa-500-plus-probuje-zmodyfikowac-podstawowe-zasady-przetwarzania-danych-osobowych.html, [dostęp: 27.04.2019]

Grabowska T., *Branżowe kodeksy postępowania i podmioty monitorujące*, https://gu.com.pl/branzowe-kodeksy-postepowania-i-podmioty-monitorujace/, [dostęp: 17.11.2020]

Greser J., *Kary za nieprzestrzeganie przepisów RODO*, https://publicystyka.ngo.pl/kary-za-nieprzestrzeganie-przepisow-rodo, [dostęp: 30.12.2020]

Grupa Robocza art. 29. Informacje ogólne, Prezes Urzędu Ochrony Danych Osobowych, https://uodo.gov.pl/pl/57, [dostęp: 01.07.2021]

Gumularz M., Kozik P., *Odpowiedzialność administracyjna przy powierzaniu*, http://www.abi-expert.pl/wydania/pazdziernikgrudzien-2017/art,1881,odpowiedzialnosc-administracyjna-przy-powierzaniu.html, [dostęp: 07.10.2020]

Horn Iwaya L., *Privacy Impact Assessment (PIA) methodology overview*, https://www.researchgate.net/figure/Privacy-Impact-Assessment-PIA-methodology-overview_fig1_330031552, [dostęp: 17.12.2020]

Informacja o przetwarzaniu danych osobowych w ramach wykonywania umowy przewozu zawartej pomiędzy pasażerem a PLL LOT S.A., https://www.lot.com/cz/pl/ochrona-danych-osobowych/klauzula-informacyjna-przewoz, [dostęp: 22.07.2021]

Inspektor Ochrony Danych – co się za tym kryje, https://evosolutions.com.pl/inspektor-ochrony-danych-co-sie-za-tym-kryje/, [dostęp: 17.12.2020]

Jak jesteśmy profilowani w sieci?, https://cyfrowa-wyprawka.org/lekcja/jak-jestesmy-profilowani-w-sieci, [dostęp: 17.12.2020]

Jak wypełnić rejestr kategorii czynności przetwarzania danych, https://www.poradyodo.pl/aktualnosci-rodo/jak-wypelnic-rejestr-kategorii-czynnosci-przetwarzania-danych-9231.html, [dostęp: 27.11.2020]

Jeśli chcesz złożyć skargę…, Urząd Ochrony Danych Osobowych, https://uodo.gov.pl/pl/83/155, [dostęp: 17.12.2020]

Kacprzak I., *Kary podetną skrzydła*, https://archiwum.rp.pl/artykul/1459898-Kary-podetna-skrzydla.html, [dostęp: 5.10.2021]

Kara dla Facebooka. „Ostrzeżenie dla każdej firmy, która uważa, że jest ponad prawem", https://www.money.pl/gospodarka/potezna-kara-dla-facebooka-ostrzezenie-dla-kazdej-firmy-ktora-uwaza-ze-jest-ponad-prawem-6695940596378208a.html, [dostęp: 30.12.2020]

Kara dla Google'a, https://ec.europa.eu/poland/news/190320_google_pl, [dostęp: 30.12.2020]

Kara rekordowej wysokości za naruszenie przepisów RODO?, https://gdpr.pl/kara-rekordowej-wysokosci-za-naruszenie-przepisow-rodo, [dostęp: 15.02.2022]

KE wszczęła postepowania antymonopolowe wobec firmy Apple, https://www.pb.pl/ke-wszczela-postepowania-antymonopolowe-wobec-firmy-apple-993943, [dostęp: 30.12.2020]

Kiedy stosujemy ustawę DODO – obowiązki z niej wynikające, https://odo24.pl/blog-post.co-w-sytuacji-gdy-rodo-nie-ma-zastosowania-czyli-obowiazywanie-przepisow-ustawy-dodo, [dostęp: 17.07.2021]

Kiedy zgoda jest uznana za ważną?, Komisja Europejska, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/when-consent-valid_pl, [dostęp: 24.11.2020]

Klauzula informacyjna – ustawa DODO, https://mazowiecka.policja.gov.pl/ra/rodododo/29123,Ochrona-danych-osobowych-przetwarzanych-w-zwiazku-z-zapobieganiem-i-zwalczaniem-.html, [dostęp: 17.07.2021]

Kmiecicka, K., *Współadministrowanie danymi osobowymi*, https://blog-daneosobowe.pl/wspoladministrowanie-danymi-osobowymi/, [dostęp: 02.12.2020]

Kodeksy postępowania muszą spełniać określone wymagania, Urząd Ochrony Danych Osobowych, https://uodo.gov.pl/pl/138/1858, [dostęp:18.08.2021]

Komunikat dotyczący nowelizacji ustawy o ochronie danych osobowych, GIODO https://archiwum.giodo.gov.pl/560/id_art/9121, [dostęp: 27.04.2020]

Kolejna kara dla Facebooka za naruszenie prywatności, https://bitdefender.pl/kolejna-kara-dla-facebooka-za-naruszenie-prywatnosci/, [dostęp: 30.12.2020]

Kolejna miliardowa kara dla Google od Unii, https://www.prawo.pl/biznes/google-ukarany-przez-ke-za-blokowanie-dostepu-konkurentom-do,389010.html, [dostęp: 30.12.2020]

Komunikat Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 sierpnia 2018 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony, https://monitorpolski.gov.pl/M2018000082701.pdf, [dostęp: 07.12.2020]

Komunikat Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 czerwca 2019 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony, https://monitorpolski.gov.pl/M2019000066601.pdf, [dostęp: 07.12.2020]

Kontrola nad danymi o przelocie pasażera (PNR), Rada Europejska, https://www.consilium.europa.eu/pl/policies/fight-against-terrorism/passenger-name-record/, [dostęp: 22.07.2021]

Krawiec W., *Co za dużo to nie RODO – ile danych osobowych naprawdę wolno przetwarzać?*, https://lassotakrawiec.pl/wiedza/co-za-duzo-to-nie-rodo-ile-danych-osobowych-naprawde-wolno-przetwarzac/, [dostęp: 13.12.2020]

Krawiel M., Jadczak S., *Miały być gigantyczne kary. Jest kapiszon. RODO po polsku*, https://www.money.pl/gospodarka/mialy-byc-gigantyczne-kary-jest-kapiszon-rodo-po-polsku-6736281656224544a.html, [dostęp: 15.02.2022]

Kulesza M., *Surowa kara dla Microsoftu*, https://codozasady.pl/p/surowa-kara-dla-microsoftu, [dostęp: 30.12.2020]

Madecki M., *Pierwszy zatwierdzony kodeks postępowania RODO*, https://rodoradar.pl/pierwszy-zatwierdzony-kodeks-postepowania-rodo/, [dostęp:18.08.2021]

Malicka M., *Podejście oparte na ryzyku czyli Risk Based Approach*, http://przetwarzaniedanych.pl/podejscie-oparte-na-ryzyku-czyli-risk-based-approach/, [dostęp: 30.05.2020]

Malujda R., *Kary za naruszenie przepisów o ochronie danych osobowych*, https://malujda.pl/kary-za-naruszenie-przepisow-o-ochronie-danych-osobowych-ochrona-danych-osobowych/, [dostęp: 30.12.2020]

Małobęcka-Szwast I., *Nowe standardowe klauzule umowne*, https://www.traple.pl/2021/06/17/nowe-standardowe-klauzule-umowne/, [dostęp: 07.07.2021]

Mamys T., *RODO: Karna i cywilna odpowiedzialność za naruszenie ochrony danych osobowych*, https://www.sage.com/pl-pl/blog/rodo-karna-i-cywilna-odpowiedzialnosc-za-naruszenie-ochrony-danych-osobowych/, [dostęp: 15.12.2020]

Metody zabezpieczeń danych osobowych oraz miejsca ich przetwarzania w Uniwersytecie Jagiellońskim, https://iod.uj.edu.pl/newsletter/-/journal_content/56_INSTANCE_xQD2n5no, [dostęp: 10.12.2020]

Michałowicz, A., *Współadministrowanie danymi osobowymi. Konsekwencje wyroku Trybunału Sprawiedliwości w sprawie C-40/17 Fashion ID*, https://www.parp.gov.pl/component/content/article/63971:wspoladministrowanie-danymi-osobowymi-konsekwencje-wyroku-trybunalu-sprawiedliwosci-w-sprawie-c-40–17-fashion-id, [dostęp: 02.12.2020]

Milan M., Naruszenie przepisów RODO a odpowiedzialność cywilnoprawna, https://poradnikprzedsiebiorcy.pl/-naruszenie-przepisow-rodo-a-odpowiedzialnosc-cywilnoprawna, [dostęp: 15.12.2020]

Monitorowanie kodeksów. Jak stworzyć odpowiedni mechanizm? Na co zwrócić uwagę a czego unikać, Urząd Ochrony Danych Osobowych, https://uodo.gov.pl/pl/138/2203, [dostęp:18.08.2021]

Nowak A., *Wymogi informatyczne RODO*, http://bezowijania.com/wymogi-informatyczne-rodo, [dostęp: 10.12.2020]

Obowiązek informacyjny w praktyce – po co, kiedy i gdzie?, GDPR.PL, Obowiązek informacyjny w praktyce – po co, kiedy i gdzie? – GDPR.pl – ochrona danych osobowych w UE, RODO, IOD, [dostęp: 29.11.2021]

Ochrona danych osobowych pracownika, czyli RODO a pracodawca, https://ipersonel.pl/baza-wiedzy-ochrona-danych-osobowych-pracownika-czyli-rodo-a-pracodawca/, [dostęp: 17.12.2020]

Ochrona osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne UE, https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=LEGISSUM:4374552, [dostęp: 20.01.2021]

Ogromna kara dla Facebooka. Musi zapłacić 5 mld dolarów. W tle afera z Cambridge Analytica, https://technologia.dziennik.pl/internet/artykuly/603447,facebook-pieniadze-kara-5-mld-dolarow.html, [dostęp: 30.12.2020]

Omówienie projektu ustawy o ochronie danych osobowych, GDPR.PL, https://gdpr.pl/omowienie-projektu-ustawy-o-ochronie-danych-osobowych, [dostęp: 02.12.2020]

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, [dostęp: 07.07.2021]

Opinion 17/2020 on the draft Standard Contractual Clauses submitted by the SI SA (Article 28(8) GDPR), European Data Protection Board, https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-172020-draft-standard-contractual-clauses_en , [dostęp: 07.07.2021]

Opinion 18/2021 on the draft Standard Contractual Clauses submitted by the LT SA (Article 28(8) GDPR), European Data Protection Board, https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-182021-draft-standard-contractual-clauses_pl, [dostęp: 07.07.2021]

Osiej, T., *Współadministrowanie danymi osobowymi – co wiemy o tej instytucji?*, https://gdpr.pl/wspoladministrowanie-danymi-osobowymi-co-wiemy-o-tej-instytucji, [dostęp: 02.12.2020]

Osowska S., *Akredytacja i certyfikacja na gruncie RODO*, https://cowprawiepiszczy.com/2019/04/akredytacja-i-certyfikacja-na-gruncie-rodo/, [dostęp: 18.08.2021]

Pierwsza opinia EROD w sprawie kryteriów certyfikacji, Urząd Ochrony Danych Osobowych, https://uodo.gov.pl/pl/138/2299, [dostęp:6.02.2022]

Ponad pół miliona złotych kary dla Santander Bank Polska. Były pracownik mógł przeglądać dane, https://businessinsider.com.pl/finanse/ponad-pol-miliona-zlotych-kary-dla-santander-bank-polska-byly-pracownik-mogl/0x4pqmh, [dostęp: 15.02.2022]

Popiel M., *Pozytywna opinia dla pierwszych kodeksów postępowania RODO,* https://panoptykon.org/pierwsze-kodeksy-rodo-zatwierdzone, [dostęp:18.08.2021]

Poradnik RODO. Podejście oparte na ryzyku. Jak rozumieć podejście oparte na ryzyku cz. 1., file:///C:/Users/adwok/Downloads/Jak%20rozumie%C4%87%20podej%C5%9Bcie%20oparte%20na%20ryzyku%20wed%C5%82ug%20RODO_.pdf, [dostęp: 17.11.2020]

Poradnik RODO. Podejście oparte na ryzyku. Jak rozumieć podejście oparte na ryzyku cz. 2., https://rodo-hr-consulting.com.pl/wp-content/uploads/2019/03/Cz%C4%99%C5%9B%C4%87–2.-Poradnik-RODO-Podej%C5%9Bcie-oparte-na-ryzyku.pdf, [dostęp: 17.11.2020]

Powierzenie przetwarzania danych a udostępnienie – różne formy przekazywania, https://blog-daneosobowe.pl/powierzenie-a-udostepnienie-danych-rozne-formy-przekazywania/, [dostęp: 14.12.2021]

Powierzenie przetwarzania danych osobowych – czym dokładnie jest i kiedy je stosujemy?, https://odo24.pl/blog-post.powierzenie-przetwarzania-danych-osobowych-czym-dokladnie-jest-i-kiedy-je-stosujemy, [dostęp: 05.11.2020]

Prezes UODO rozpoczyna konsultacje dotyczące umów powierzenia przetwarzania danych, https://uodo.gov.pl/pl/138/650, [dostęp: 07.07.2021]

Prezes UODO wyjaśnia, jak przekazywać dane osobowe z Polski do Wielkiej Brytanii na wypadek Brexitu, https://uodo.gov.pl/pl/138/665, [dostęp: 06.12.2020]

Procedura zatwierdzania kodeksu, Urząd Ochrony Danych Osobowych, https://uodo.gov.pl/pl/426/1103, [dostęp:18.08.2021]

Program 500+ a ochrona danych osobowych, https://blog-daneosobowe.pl/program-500-a-ochrona-danych-osobowych/, [dostęp: 27.04.2020]

Program 500+ a ochrona danych osobowych, http://wartowiedziec.pl/polityka-spoleczna/30128-program-500-a-ochrona-danych-osobowych, [dostęp: 27.04.2020]

Projekt ustawy o ochronie danych osobowych, https://legislacja.rcl.gov.pl/projekt/12302950, [dostęp: 12.12.2020]

Projekt ustawy o ochronie danych osobowych skierowany na Komitet do Spraw Europejskich Rady Ministrów, https://www.gov.pl/web/cyfryzacja/projekt-ustawy-o-ochronie-danych-osobowych-skierowany-na-komitet-do-spraw-europejskich-rady-ministrow, [dostęp: 02.12.2020]

Projekt ustawy o ochronie danych osobowych z dnia 28 marca 2017 roku, https://www.gov.pl/web/cyfryzacja/projekt-ustawy-o-ochronie-danych-osobowych, [dostęp: 05.12.2021]

Projekt ustawy o ochronie danych osobowych z 12 września 2017 r., https://odoserwis.pl/a/1149/projekt-ustawy-o-ochronie-danych-osobowych-z-dnia-12-wrzesnia-2017-r, [dostęp: 05.12.2021]

Projekt ustawy o ochronie danych osobowych z marca 2017, https://mc.gov.pl/files/projekt_ustawy_o_ochronie_danych_osobowych_28.03.2017.pdf, [dostęp: 30.05.2020]

Projekt wytycznych Europejskiej Rady Ochrony Danych osobowych w sprawie transferu danych poza UE został opublikowany, https://legalis.pl/projekt-wytycznych-europejskiej-rady-ochrony-danych-osobowych-w-sprawie-transferu-danych-poza-ue-zostal-opublikowany/, [dostęp: 11.12.2020]

Przekazywanie danych osobowych do państw trzecich zgodnie z RODO... czyli jak?, https://blog-daneosobowe.pl/przekazywanie-danych-osobowych-do-panstw-trzecich-zgodnie-z-rodo/, [dostęp: 10.12.2020]

Przekazywanie danych do USA ponownie pod znakiem zapytania, https://gdpr.pl/aktualnosci/przekazywanie-danych-do-usa-ponownie-pod-znakiem-zapytania, [dostęp: 07.12.2020]

Przetwarzanie danych na podstawie prawnie uzasadnionego interesu, https://lexdigital.pl/przetwarzanie-danych-na-podstawie-uzasadnionego-interesu, [dostęp: 13.12.2020]

Rapcewicz, A., *Kilka słów o współadministrowaniu danymi osobowymi*, iSecure, https://www.isecure.pl/blog/kilka-slow-o-wspoladministrowaniu-danymi-osobowymi/, [dostęp: 02.12.2020]

Rejestrowanie czynności przetwarzania, Poradnik Prezesa UODO, https://uodo.gov.pl/pl/123/214, [dostęp: 27.11.2020]

Rekomendacja Nr 06/2017 z 14 czerwca 2017 r. wydana przez belgijski urząd ochrony danych osobowych (Komisja ds. Prywatności), https://www.gegevensbeschermingsautoriteit.be/publications/recommandation-n-06–2017.pdf, [dostęp: 18.10.2020]

Rekordowa kara dla Google. Komisja Europejska nakazuje zapłacić aż 4,3 mld euro, https://www.money.pl/gospodarka/unia-europejska/wiadomosci/artykul/kara-dla-google-komisja-europejska-android,85,0,2411349.html, [dostęp: 30.12.2020]

Risk Based Approach To Cyber And Information Security, https://www.slideteam.net/risk-based-approach-to-cyber-and-information-security.html, [dostęp: 17.12.2021]

RODO i kary za wyciek danych – jak uniknąć ryzyka dzięki Microsoft Business 365?, https://blog.home.pl/2018/11/rodo-i-kary-za-wyciek-danych-jak-uniknac-ryzyka-dzieki-microsoft-business-365/, [dostęp: 30.12.2020]

RODO na tacy. Odcinek V: Lekcje samoobrony, czyli jak skorzystać z praw, które daje RODO?, https://panoptykon.org/rodo-na-tacy-V, [dostęp: 15.11.2020]

RODO: Pierwsza kara za wyciek danych w następstwie ataku z zewnątrz, https://www2.deloitte.com/pl/pl/pages/doradztwo-prawne/articles/ochrona-danych-osobowych/newsletter-rodo0/RODO-pierwsza-kara-za-wyciek-danych-w-nastepstwie-ataku-z-zewnatrz.html, [dostęp: 30.12.2020]

RODO: Przekazywanie danych osobowych do państw trzecich. Czyli co każdy administrator powinien sprawdzić przed dokonaniem transferu, https://www2.deloitte.com/pl/pl/pages/doradztwo-prawne/articles/ochrona-danych-osobowych/newsletter-rodo0/RODO-przekazywanie-danych-osobowych-do-panstw-trzecich.html, [dostęp: 11.12.2020]

RODO zabezpieczenia techniczne systemów informatycznych, https://www.spark-it.pl/blog/rodo-zabezpieczenia-techniczne-systemow-informatycznych/, [dostęp: 10.12.2020]

Rychły G., *Administracyjne kary pieniężne nakładane przez PUODO*, https://mojafirma.infor.pl/biznes/prawo/rodo-w-firmie/3101901,Administracyjne-kary-pieniezne-nakladane-przez-PUODO.html, [dostęp: 15.12.2020]

Rząd przyjął projekt zmian w ustawie o przetwarzaniu danych dotyczących przelotu pasażera, https://www.gov.pl/web/mswia/rzad-przyjal-projekt-zmian-w-ustawie-o-przetwarzaniu-danych-dotyczacych-przelotu-pasazera, [dostęp: 22.07.2021]

Rządowy projekt ustawy o ochronie danych osobowych, druk 2410, https://www.sejm.gov.pl/sejm8.nsf/PrzebiegProc.xsp?nr=2410, [dostęp: 12.12.2020]

Rządowy projekt ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, druk 2989, https://www.sejm.gov.pl/Sejm8.nsf/PrzebiegProc.xsp?nr=2989, [dostęp: 17.07.2021]

Rzemek M., *4,9 mln zł – nowy rekord kary za naruszenie RODO*, https://www.rp.pl/dane-osobowe/art35775391–4-9-mln-zl-nowy-rekord-kary-za-naruszenie-rodo, [dostęp: 15.02.2022]

Sejm znowelizował ustawę o przetwarzaniu danych, dotyczących przelotu pasażera, https://inwestycje.pl/gospodarka/sejm-znowelizowal-ustawe-o-przetwarzaniu-danych-dotyczacych-przelotu-pasazera/, [dostęp: 22.07.2021]

Skibińska A., *Jak prezes UODO nakłada administracyjne kary pieniężne?*, https://www.politykabezpieczenstwa.pl/pl/a/jak-prezes-uodo-naklada-administracyjne-kary-pieniezne, [dostęp: 19.12.2020]

Sobczak K. *RODO – certyfikacja to obowiązek i korzyści dla administratora danych*, https://www.prawo.pl/prawnicy-sady/rodo-certyfikacja-to-obowiazek-i-korzysci-dla-administratora-danych,74396.html, [dostęp: 18.08.2021]

Sobczak K., *RODO: Osiem projektów kodeksów, ale żaden jeszcze nie zatwierdzony*, https://www.prawo.pl/biznes/kodeksy-rodo-osiem-projektow-ale-zaden-jeszcze-nie-zatwierdzony,505991.html, [dostęp:18.08.2021]

Sobczak K.,*, Siedmiokrotny wzrost kar za naruszenie RODO w Europie*, https://www.prawo.pl/prawo/kary-za-naruszenie-rodo-w-europie-duzy-wzrost,512924.html, [dostęp: 15.02.2022]

Sobkowicz M., *Kary za nieprzekazanie danych dotyczących przelotu pasażera (PNR)*, https://codozasady.pl/p/kary-za-nieprzekazanie-danych-dotyczacych-przelotu-pasazera-pnr-, [dostęp: 22.07.2021]

Stanowisko GIODO w sprawie zachowania ważności zgód na przetwarzanie danych, odnoszące się do dyskusji publicznej na ten temat, opiera się na Wytycznych Grupy Roboczej art. 29

dotyczących zgody na mocy rozporządzenia 2016/679 (WP259), https://archiwum.giodo.gov.pl/pl/1520281/10303, [dostęp: 24.11.2020]

Stępniewski R. *Jak ocenić ryzyko naruszenia praw lub wolności osób fizycznych na wypadek stwierdzenia naruszenia?*, https://www.politykabezpieczenstwa.pl/pl/a/jak-ocenic-ryzyko-naruszenia-praw-lub-wolnosci-osob-fizycznych-na-wypadek-stwierdzenia-naruszenia, [dostęp: 13.12.2020]

Stępniewski R., *Ocena skutków przetwarzania – komunikat PUODO*, https://www.politykabezpieczenstwa.pl/pl/a/ocena-skutkow-przetwarzania-komunikat-puodo, [dostęp: 18.11.2020]

Szczypińska K., *RODO: Wysokie wymagania wobec podmiotów certyfikujących*, https://www.prawo.pl/biznes/wymogi-erod-dla-podmiotow-certyfikujacych-katarzyna-szczypinska,366145.html, [dostęp: 17.11.2020]

Szkutnik M., *Przepisy o ochronie danych osobowych, czyli nie tylko RODO*, https://blog-daneosobowe.pl/przepisy-o-ochronie-danych-osobowych-czyli-nie-tylko-rodo/, [dostęp: 17.07.2021]

Szykuj się do RODO! Kiedy i jaka zgoda na przetwarzanie danych osobowych, https://poradnik.ngo.pl/c-szykuj-sie-do-rodo-kiedy-i-jaka-zgoda-na-przetwarzanie-danych-osobowych, [dostęp: 24.11.2020]

Szymielewicz K., *Śledzenie i profilowanie w sieci: W czym problem? Co się zmieni w prawie? Jak może wyglądać przyszłość?*, Fundacja Panoptykon, wrzesień 2017, https://panoptykon.org/sites/default/files/publikacje/sledzenie_i_profilowanie_w_sieci_scenariusze_po_reformie_ue_wrzesien_2017.pdf, [dostęp: 30.12.2020]

Tchórzewska B., *Zbiór danych osobowych dzisiaj i według RODO, https://blog-daneosobowe.pl/zbior-danych-osobowych-charakterystyka-pojecia/*, [dostęp: 17.11.2020]

Topolewska M., *500+ a RODO: Rodzice jednak muszą zostać poinformowani o przetwarzaniu danych osobowych*, https://prawo.gazetaprawna.pl/artykuly/1159736,przetwarzanie-danych-osobowych-a-500.html, [dostęp: 27.04.2020]

Transfer danych do państw trzecich zgodny z RODO, https://uodo.gov.pl/pl/138/2085, [dostęp: 07.07.2021]

Transfer danych osobowych, https://blog-daneosobowe.pl/wp-content/uploads/2020/12/lex_infografika_transfer_panstwo_trzecie.png, [dostęp: 12.12.2020]

Transfer danych osobowych poza Europejski Obszar Gospodarczy, https://odoserwis.pl/a/1243/transfer-danych-osobowych-poza-europejski-obszar-gospodarczy-eog, [dostęp: 09.12.2021]

Trustwave Global Security Report, https://www2.trustwave.com/rs/815-RFM-693/images/2015 TrustwaveGlobalSecurityReport.pdf, [dostęp: 05.12.2020]

Turek A., *Google to nie wszystko. Największe kary antymonopolowe dla technologicznych gigantów w historii UE*, https://businessinsider.com.pl/firmy/zarzadzanie/kary-antymonopolowe-od-komisji-europejskiej-google-to-nie-wszystko/6z9216z, [dostęp: 30.12.2020]

UE nałożyła na Microsoft 561 mln euro kary. Za przeglądarkę, https://www.forbes.pl/technologie/ue-nalozyla-na-microsoft-561-mln-euro-kary-za-przegladarke/xeyd882, [dostęp: 30.12.2020]

Unia bije w Amazona. Rekordowa kara za naruszenie RODO, https://cyfrowa.rp.pl/globalne-interesy/art18547121-unia-bije-w-amazona-rekordowa-kara-za-naruszenie-rodo, [dostęp: 30.07.2021]

Unia Europejska grilluje Facebooka. Nasze dane mogły być wykorzystywane do nieuczciwej konkurencji, https://www.money.pl/gospodarka/unia-europejska-grilluje-facebooka-ke-wszczyna-sledztwo-6648040035318432a.html, [dostęp: 30.12.2020]

Ustawa wdrażająca dyrektywę 2016/680, zwana potocznie „policyjną", już obowiązuje, https://uodo.gov.pl/pl/138/706, [dostęp: 17.07.2021]

Uzasadnienie do rządowego projektu ustawy o zmianie ustawy o ochronie danych osobowych, druk sejmowy Nr 2120, Sejm IV kadencji, s. 20, https://www.sejm.gov.pl/sejm8.nsf/PrzebiegProc.xsp?nr=2410, [dostęp: 15.05.2020]

Wikariak S., *Rekordowa kara za naruszenie RODO*, https://www.gazetaprawna.pl/firma-i-prawo/artykuly/8369936,naruszenie-rodo-kary-fortum-marketing-and-sales-polska.html, [dostęp: 15.02.2022]

Wniosek dotyczący dyrektywy Parlamentu Europejskiego i Rady w sprawie wykorzystania danych dotyczących przelotu pasażera w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia dochodzeń w ich sprawie i ich ścigania, Komisja Europejska, 3.02.2011, 2011/0023 (COD), 6007/11, Justice and fundamental rights | European Commission, http://ec.europa.eu/justice/data-protection/reform/index_en.htm, [dostęp: 05.05.2020]

Wniosek dotyczący dyrektywy Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez właściwe organy do celów zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich i ścigania albo wykonywania kar kryminalnych oraz swobodnego przepływu tych danych, COM(2012) 10 final z 25.1.2012, Justice and fundamental rights | European Commission, http://ec.europa.eu/justice/data-protection/reform/index_en.htm, [dostęp: 05.05.2020]

Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych), COM(2012) 11 final z 25.1.2012, Justice and fundamental rights | European Commission, http://ec.europa.eu/justice/data-protection/reform/index_en.htm, [dostęp: 05.05.2020]

Wolska A., *Francja: Google ukarany za działania w sferze reklamowej. Zapłaci 220 mln euro grzywny*, https://www.euractiv.pl/section/gospodarka/news/francja-google-ukarany-za-dzialania-w-sferze-reklamowej-zaplaci-220-mln-euro-grzywny/, [dostęp: 30.12.2020]

Wrodarczyk W., *Pseudonimizacja danych osobowych w marketingu online*, https://adequate.digital/web-analytics/pseudonimizacja-danych-osobowych-marketingu-online, [dostęp: 17.12.2020]

Wskazówki i wyjaśnienia dotyczące obowiązku rejestrowania czynności i kategorii czynności przetwarzania określonego w art. 30 ust. 1 i 2 RODO, Urząd ds. Ochrony Danych Osobowych, file:///C:/Users/

adwok/Downloads/Wskaz%C3%B3wki%20i%20wyja%C5%9Bnienia%20dotycz%C4%85ce%20obowi%C4%85zku%20z%20art.%2030%20ust.%201%20i%202%20RODO.pdf, [dostęp: 21.11.2020]

Współpraca międzynarodowa, Urząd Ochrony Danych Osobowych, https://uodo.gov.pl/p/wspolpraca, [dostęp: 01.07.2021]

W*spółpraca na rzecz wzmocnienia praw. Streszczenie sprawozdania rocznego za rok 2019*, Europejska Rada Ochrony Danych,https://edpb.europa.eu/sites/default/files/files/file2/edpb_annual_report_2019_-_digital_summary_pl.pdf, [dostęp: 15.07.2021]

Wyrok Trybunału Sprawiedliwości Unii Europejskiej z 6 października 2015 r. w sprawie Maximillian Schrems p-ko Data Protection Commissioner, tzw. Schrems I, (C-362/14), https://sip.lex.pl/orzeczenia-i-pisma-urzedowe/orzeczenia-sadow/c-362–14-maximillian-schrems-v-data-protection-522014682, [dostęp: 07.12.2020]

Wyrok Trybunału Sprawiedliwości Unii Europejskiej z 5 czerwca 2018 roku (C-210/16), https://curia.europa.eu/juris/document/document.jsf;jsessionid=7C7F5AF47195D4A7611D87976D8765C4?text=&docid=202543&pageIndex=0&doclang=pl&mode=lst&dir=&occ=first&part=1&cid=8224414, [dostęp: 02.12.2020]

Wyrok Trybunału Sprawiedliwości Unii Europejskiej z 29 lipca 2019 roku (C-40/17), https://curia.europa.eu/juris/document/document.jsf?text=&docid=216555&doclang=PL, [dostęp: 02.12.2020]

Wyrok Trybunału Sprawiedliwości Unii Europejskiej z 16 lipca 2020 r. TSUE w sprawie Data Protection Commissioner przeciwko Facebook Ireland Ltd. i Maximilian Schrems, tzw. Schrems II, (C-311/18), https://sip.lex.pl/orzeczenia-i-pisma-urzedowe/orzeczenia-sadow/c-311–18-przekazywanie-danych-obywateli-panstw-523123145, [dostęp: 07.12.2020]

Wystąpienie do Generalnego Inspektora Ochrony Danych Osobowych ws. ochrony danych osobowych w związku z realizacją programu Rodzina 500 plus, https://www.rpo.gov.pl/pl/content/wystapienie-do-giodo-ws-ochrony-danych-osobowych-w-zwiazku-z-realizacja-programu-500-plus, [dostęp: 27.04.2019]

Wytyczne 2/2018 w sprawie wyjątków określonych w art. 49 rozporządzenia 2016/679, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_pl, [dostęp: 12.12.2020]

Wytyczne dotyczące ustalenia wiodącego organu nadzorczego właściwego dla administratora lub podmiotu przetwarzającego (WP 244), https://www.uodo.gov.pl/pl/10/5, [dostęp: 17.11.2020]

Wytyczne dotyczące zgody na mocy rozporządzenia 2016/679, przyjęte 28 listopada 2017 r. (17/PL WP259), http://giodo.gov.pl/pl/1520281/10292, [dostęp: 24.11.2020]

Wytyczne EROD w sprawie przesyłania danych do państw trzecich, https://gdpr.pl/wytyczne-erod-w-sprawie-przesylania-danych-do-panstw-trzecich, [dostęp: 10.12.2020]

Wytyczne dotyczące ustalenia wiodącego organu nadzorczego właściwego dla administratora lub podmiotu przetwarzającego (WP 244), https://www.uodo.gov.pl/pl/10/5, [dostęp: 17.11.2020]

Złożone wnioski o zatwierdzenie kodeksów, Urząd Ochrony Danych Osobowych, https://uodo.gov.pl/pl/426/1109, [dostęp:18.08.2021]

Znika obowiązek rejestracji zbiorów w GIODO w zamian obowiązek rejestrowania czynności przetwarzania, https://odo24.pl/blog-post.znika-obowiazek-rejestracji-zbiorow-w-giodo-w-zamian-obowiazek-rejestrowania-czynnosci-przetwarzania2, [dostęp: 19.10.2020]

SPIS DOKUMENTACJI SYSTEMU OCHRONY DANYCH

Polityka Ochrony Danych Osobowych

1) Upoważnienie do przetwarzania danych osobowych – wzór
2) Anulowanie Upoważnienia do przetwarzania danych osobowych – wzór
3) Rejestr osób upoważnionych – wzór
4) Upoważnienie do przebywania w obszarze przetwarzania – wzór
5) Powołanie Inspektora Ochrony Danych – wzór
6) Anulowanie powołania Inspektora Ochrony Danych – wzór
7) Oświadczenie Inspektora Ochrony Danych – wzór
8) Przykłady zgód i klauzul informacyjnych – wzór
9) Polityka retencyjna – wzór
10) Opis zabezpieczeń fizycznych, technicznych i programowych – wzór
11) Rejestr podmiotów zewnętrznych, którym powierzono przetwarzanie danych – wzór
12) Protokół z czynności audytowych w zakresie ochrony danych – wzór
13) Sprawozdanie z kontroli zgodności przetwarzania danych – wzór
14) Oświadczenie pracownika o zobowiązaniu się do przestrzegania zasad ochrony – wzór
15) Umowna klauzula zachowania ochrony danych – wzór
16) Protokół usunięcia danych osobowych – wzór
17) Protokół przekazania dokumentów w związku w prowadzoną kontrolą – wzór
18) Instrukcja zarządzania kluczami – wzór
19) Instrukcja zarządzania naruszeniami – wzór
20) Analiza ryzyka – metodologia – wzór

Instrukcja Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych

1) Nadanie uprawnień w systemie informatycznym – wzór
2) Przekazanie parametrów uwierzytelnienia – wzór
3) Rejestr użytkowników i uprawnień w systemie – wzór
4) Powołanie Administratora Systemu Informatycznego – wzór
5) Anulowanie powołania Administratora Systemu Informatycznego – wzór
6) Oświadczenie Administratora Systemu Informatycznego – wzór
7) Rejestr mobilnych nośników danych – wzór
8) Rejestr incydentów informatycznych – wzór
9) Oświadczenie o wzięciu udział w szkoleniu informatycznym – wzór
10) Dziennik Administratora Systemu Informatycznego – wzór

SPIS ZAŁĄCZNIKÓW

1) Komunikat Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 czerwca 2019 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony (M.P. 2019 poz. 666)
2) Zawiadomienie o wyznaczeniu nowego Inspektora Ochrony Danych (RODO) – formularz
3) Zawiadomienie o odwołaniu dotychczasowego Inspektora Ochrony Danych i wyznaczenie nowego (DODO) – formularz
4) Zgłoszenie naruszenia ochrony danych osobowych – formularz
5) Oświadczenie w sprawie wyrażenia zgody na przetwarzanie danych osobowych – wzór
6) Wniosek o usunięcie danych osobowych (prawo do bycia zapomnianym) – wzór
7) Umowa powierzenia przetwarzania danych osobowych – wzór
8) Umowa udostępnienia danych osobowych – wzór
9) Decyzja wykonawcza Komisji (UE) 2021/914 z dnia 4 czerwca 2021 r. w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 (Tekst mający znaczenie dla EOG), Dz.Urz. L UE 199/31 z 7.6.2021r.
10) Decyzja wykonawcza Komisji (UE) (UE) 2021/915 z dnia 4 czerwca 2021 r. w sprawie standardowych klauzul umownych między administratorami a podmiotami przetwarzającymi na podstawie art. 28 ust. 7 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 oraz art. 29 ust. 7 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 (Tekst mający znaczenie dla EOG), Dz.Urz. L UE 199/31 z 7.6.2021r.
11) Opinia 17/2018 w sprawie projektu wykazu sporządzonego przez właściwy polski organ nadzorczy dotyczącego rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych (art. 35 ust. 4 RODO), przyjęta 25 września 2018 r., Europejska Rada Ochrony Danych
12) Opinia 31/2020 w sprawie projektu decyzji właściwego organu nadzorczego Polski w sprawie zatwierdzenia wymogów akredytacji podmiotu monitorującego przestrzeganie kodeksu postępowania zgodnie z art. 41 (RODO), przyjęta 7 grudnia 2020 r., Europejska Rada Ochrony Danych
13) Komunikat Komisji do PE i Rady Wzmocniona ochrona, nowe możliwości – wytyczne Komisji dotyczące bezpośredniego stosowania ogólnego rozporządzenia o ochronie danych od dnia 25 maja 2018 r., Bruksela, 24.1.2018r. COM(2018) 43 final
14) Komunikat Komisji do PE i Rady Ochrona danych jako filar wzmacniania pozycji obywateli oraz podejścia UE do transformacji cyfrowej – dwa lata stosowania ogólnego rozporządzenia o ochronie danych [SWD(2020) 115 final], Bruksela, 24.6.2020 r. COM(2020) 264 final

DOKUMENTACJA SYSTEMU OCHRONY DANYCH – WYBRANE WZORY

	POLITYKA OCHRONA DANYCH OSOBOWYCH	Wersja	1.00
		Data opracowania	……..
		Właściciel	……..
UPOWAŻNIENIE DO PRZETWARZANIA DANYCH – WZÓR			Załącznik nr 1

. . . . . .

(miejscowość, data)

Upoważnienie Nr ……

do przetwarzania danych osobowych oraz obsługi systemu informatycznego i urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych

Działając jako Administrator Danych, niniejszym, na mocy art. 32 ust. 1 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) dalej jako „RODO" z dniem . . . . . ,

upoważniam

Panią/Pana* . . . . . .

do przetwarzania danych osobowych w następujących procesach i w następujących zakresach:

LP.	NAZWA PROCESU	ZAKRES CZYNNOŚCI PRZETWARZANIA	FORMA PRZETWARZANIA	SYSTEM INFORMATYCZNY
1.	.....	☐ zbieranie ☐ utrwalanie ☐ organizowanie ☐ porządkowanie ☐ przechowywanie ☐ adaptowanie ☐ modyfikowanie ☐ pobieranie ☐ przeglądanie ☐ wykorzystywanie ☐ ujawnianie przez przesłanie ☐ udostępnianie ☐ dopasowywanie ☐ łączenie ☐ ograniczanie ☐ usuwanie ☐ niszczenie	* papierowa * elektroniczna	
2.	.....	☐ zbieranie ☐ utrwalanie ☐ organizowanie ☐ porządkowanie ☐ przechowywanie ☐ adaptowanie ☐ modyfikowanie ☐ pobieranie ☐ przeglądanie ☐ wykorzystywanie ☐ ujawnianie przez przesłanie ☐ udostępnianie ☐ dopasowywanie ☐ łączenie ☐ ograniczanie ☐ usuwanie ☐ niszczenie	* papierowa * elektroniczna	

Zobowiązuję Panią/Pana do przestrzegania przepisów i reguł dotyczących ochrony danych osobowych oraz wdrożonych do stosowania u Administratora, w tym Polityki Ochrony Danych Osobowych.

Integralną częścią Upoważnienia, w przypadku zbioru danych przetwarzanych w systemie informatycznym, o których mowa powyżej jest Przekazania parametrów uwierzytelniania w systemie (Identyfikator).

Osoba upoważniona zobowiązuje się do przetwarzania danych osobowych zgodnie z udzielonym upoważnieniem oraz z przepisami 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), ustawy o ochronie danych osobowych, wydanymi na jej podstawie aktami wykonawczymi i obowiązującymi u Administratora wewnętrznymi regulacjami. Naruszenie ww. obowiązków może skutkować poniesieniem odpowiedzialności karnej na podstawie przepisów określonych w ww. ustawie, cywilnej oraz stanowi ciężkie naruszenie obowiązków pracowniczych, które może być podstawą do rozwiązania umowy o pracę w trybie art. 52 ustawy z 26 czerwca 1974r. Kodeks Pracy.

Osoba upoważniona do przetwarzania danych osobowych jest zobowiązana do zachowania w tajemnicy danych osobowych i sposobu ich zabezpieczenia również po odwołaniu/anulowaniu upoważnienia, a także ustaniu stosunku pracy/rozwiązaniu umowy/zakończeniu realizacji zadań związanych z przetwarzaniem danych osobowych.

Upoważnienie jest ważne do odwołania/anulowania.

ADMINISTRATOR DANYCH:	OSOBA UPOWAŻNIONA:
.....	.....
(data i podpis)	(data i podpis)

* niepotrzebne skreślić

	POLITYKA OCHRONA DANYCH OSOBOWYCH	Wersja	1.00
		Data opracowania	……...
		Właściciel	……...
ANULOWANIE UPOWAŻNIENIA DO PRZETWARZANIA DANYCH – WZÓR			Załącznik nr 2

. . . . . .

(miejscowość, data)

Anulowanie Upoważnienie Nr ……

do przetwarzania danych osobowych oraz obsługi systemu informatycznego
i urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych

Działając jako Administrator Danych, niniejszym, na mocy art. 32 ust. 1 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) dalej jako „RODO" z dniem . . . . . ,

Anuluję Upoważnienie Nr …… dla

Panią/Pana* . . . . . .

do przetwarzania danych osobowych w następujących procesach i w następujących zakresach:

. . . . . .

1				
2				

Osoba upoważniona do przetwarzania danych osobowych jest zobowiązana do zachowania w tajemnicy danych osobowych i sposobu ich zabezpieczenia również po odwołaniu/anulowaniu upoważnienia, a także ustaniu stosunku pracy/rozwiązaniu umowy/zakończeniu realizacji zadań związanych z przetwarzaniem danych osobowych.

ADMINISTRATOR DANYCH: OSOBA UPOWAŻNIONA:

…… ……

(data i podpis) (data i podpis)

* niepotrzebne skreślić

	POLITYKA OCHRONA DANYCH OSOBOWYCH	Wersja	1.00
		Data opracowania	……..
		Właściciel	……..
REJESTR OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH – WZÓR			Załącznik nr 3

Rejestr osób upoważnionych do przetwarzania danych osobowych

Lp.	Imię/Imiona Nazwisko	Status prawny	Data i nr upoważnienia	Data anulowania upoważnienia	Nazwa procesu (zakres czynności w procesie)	Nazwa systemu
1.		Pracownik* Osoba zatrudniona na podstawie umowy cywilno-prawnej* Stażysta/ praktykant/wolontariusz* Korporacja*	Np. 25 maja 2018 r. (nr 1)		▪ Prowadzenie strony internetowej – panel administracyjny ▪ Prowadzenie procesów kadrowo-pracowniczych (Wykonywanie obowiązków pracodawcy wobec pracownika) (a) Akta osobowe (b) Umowy (c) Lista płac (d) Deklaracje zgłoszenia pracowników do ZUS (e) Deklaracje przystąpienia do dodatkowego ubezpieczenia (f) Informacje roczne PIT-11 (g) Wnioski urlopowe (h) Lista pracowników delegowanych na pobyty zewnętrzne/szkolenia zewn. (i) Informacje do ubezpieczyciela pracowników wyjeżdżających (j) Rejestr postępowań dyscyplinarnych (k) Rejestr pracowników należących do związku zawodowego Prowadzenie procesów rekrutacyjnych/naborów ▪ Prowadzenie procesów księgowo-finansowych (a) Faktury (b) Przelewy (c) Prowadzenie ewidencji zaświadczeń do banków ▪ Prowadzenie dokumentacji BHP (d) Szkolenia BHP (e) Protokoły powypadkowe ▪ Prowadzenie dokumentacji systemów informatycznych ▪ Prowadzenie szkoleń wewnętrznych ▪ Prowadzenie wykazu osób upoważnionych do informacji niejawnych, oraz osób którym odmówiono wydania poświadczenia bezpieczeństwa lub je cofnięto ▪ Prowadzenie korespondencji mailowej wewnętrznej i zewnętrznej ▪ Prowadzenie ewidencji korespondencji ▪ Prowadzenie ewidencji delegacji i wyjazdów służbowych ▪ Prowadzenie relacji z podmiotami zewnętrznymi, w tym z kontrahentami handlowymi ▪ Prowadzenie postępowań przetargowych/ ofertowych/ o zamówienie ▪ Prowadzenie ewidencji uczestników konferencji ▪ Prowadzenie ewidencji postępowań administracyjnych ▪ Prowadzenie ewidencji postępowań sądowych ▪ Prowadzenie ewidencji dokumentacji związanej z nieruchomościami Administratora ▪ Prowadzenie ewidencji dłużników Administratora ▪ Prowadzenie księgi wejść i wyjść ▪ Prowadzenie rejestru gości ▪ Prowadzenie rejestru zapisów monitoringi ▪ Prowadzenie rejestru skarg i wniosków	▪ System urządzeń końcowych ▪ Poczta zewnętrzna ▪ Panel administracyjny strony internetowej Administratora ▪ Notes ▪ Xpertis (a) Środki trwałe (b) Wystawianie FV nieprojektowych (c) Finanse (d) Bankowość elektroniczna (e) Informacja finansowa (f) Kadry i płace (g) Kasa ▪ System przechowywania i wersjonowania dokumentów ▪ System kontroli dostępu ▪ Accard MP ▪ (b) Accard 2.11d ▪ PKZP ▪ Płatnik ▪ System eksportu i importu danych (TEST) ▪ MF.GOV.PL (w zakresie danych wprowadzanych) ▪ PZU.PL (w zakresie danych wprowadzanych) ▪ POLMED.PL (w zakresie danych wprowadzanych) ▪ ZUS.GOV.PL (w zakresie danych wprowadzanych) ▪ POLON.NAUKA.GOV.PL (w zakresie danych wprowadzanych) ▪ PKO S.A. (w zakresie danych wprowadzanych) ▪ ALIOR (w zakresie danych wprowadzanych)
2.		Pracownik* Osoba zatrudniona na podstawie umowy cywilno-prawnej* Stażysta/praktykant/wolontariusz* Korporacja*	Np. 25 maja 2018 r. (Nr 2)			

	POLITYKA OCHRONA DANYCH OSOBOWYCH	Wersja	1.00
		Data opracowania	……..
		Właściciel	……..
UPOWAŻNIENIE DO PRZEBYWANIA W OBSZARZE PRZETWARZANIA DANYCH – WZÓR			Załącznik nr 4

. . . . . .

(miejscowość, data)

Upoważnienie Nr ……

do przybywania w obszarze przetwarzania danych osobowych

Działając jako Administrator Danych, z dniem . . . . . ,

upoważniam

Panią/Pana* . . . . . .

do przebywania w obszarze przetwarzania danych osobowych w celu . . . . . .

w następujących procesach i w następujących zakresach:

Zobowiązuję Panią/Pana do przestrzegania przepisów i reguł dotyczących ochrony danych osobowych oraz wdrożonych do stosowania u Administratora, w tym Polityki Ochrony Danych Osobowych.

1				
2				

Upoważnienie jest ważne do odwołania/anulowania.

ADMINISTRATOR DANYCH: OSOBA UPOWAŻNIONA:

…… ……

(data i podpis) (data i podpis)

* niepotrzebne skreślić

	POLITYKA OCHRONA DANYCH OSOBOWYCH	Wersja	1.00
		Data opracowania	……..
		Właściciel	……..
POWOŁANIE INSPEKTORA OCHRONY DANYCH – WZÓR			Załącznik nr 5

. . . . . .

(miejscowość, data)

Powołanie
Inspektora Ochrony Danych

Działając jako Administrator Danych, niniejszym, na mocy art. 37 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) dalej jako „RODO" z dniem . . . . . .

powołuję/wyznaczam

Panią/Pana* . . . . . .

na stanowisko Inspektora Ochrony Danych

w . . . . . .

Zakres obowiązków oraz warunki pełnienia funkcji Inspektora Ochrony Danych określone są 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), w ustawie o ochronie danych osobowych, w przepisach do niej wykonawczych oraz w dokumentacji ochrony danych osobowych Administratora w szczególności Polityce Ochrony Danych Osobowych, z treścią których Inspektor Ochrony Danych ma obowiązek się zapoznać.

. . . . . .

(data i podpis osoby reprezentującej

Administratora Danych)

Przyjmuję

. . . . . .

(data i podpis Inspektora Ochrony Danych)

* niepotrzebne skreślić

	POLITYKA OCHRONA DANYCH OSOBOWYCH	Wersja	1.00
		Data opracowania	……..
		Właściciel	……..
ANULOWANIE POWOŁANIA INSPEKTORA OCHRONY DANYCH – WZÓR			Załącznik nr 6

. . . . . .

(miejscowość, data)

Anulowanie Powołania Inspektora Ochrony Danych

Działając jako Administrator Danych, niniejszym z dniem . . . . . .
anuluję powołanie/wyznaczenia Pani/Pana*

. . . . . .

. . . . . .

na stanowisko Inspektora Ochrony Danych w . . . . . .

. . . . . .

(data i podpis osoby reprezentującej

Administratora Danych)

Potwierdzam

. . . . . .

(data i podpis Inspektora Ochrony Danych)

* niepotrzebne skreślić

	POLITYKA OCHRONA DANYCH OSOBOWYCH	Wersja	1.00
		Data opracowania	……..
		Właściciel	……..
OŚWIADCZENIE INSPEKTORA OCHRONY DANYCH – WZÓR			Załącznik nr 7

. . . . . .

(miejscowość, data)

Oświadczenie Inspektora Ochrony Danych

Ja niżej podpisany . . . . . ,

zam. . . . . ,

Nr Pesel: . . . . . ,

oświadczam, iż:

1. posiadam kwalifikacje zawodowe, a w szczególności fachową wiedzę na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętność wypełnienia powierzonych mi zadań Inspektora Ochrony Danych;
2. zobowiązuję się do niezwłocznego poinformowania Administratora Danych o zmianie okoliczności objętych niniejszym oświadczeniem;
3. zobowiązuje się wypełniać z należytą starannością oraz z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania, m.in. następujące zadania:
   a) informowanie Administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy 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), (Dz.U.UE.L.2016.119.1), (dalej: „RODO" lub „rozporządzenie") oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
   b) monitorowanie przestrzegania rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk, procedur, instrukcji Administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
   c) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 rozporządzenia;
   d) współpraca z organem nadzorczym;
   e) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 Rozporządzenia, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach;

f) kontaktowanie się z osobami, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy Rozporządzenia;
g) przygotowywanie dla Administratora, co najmniej raz w roku, pisemnego sprawozdania ze swojej działalności;
h) nadzorowanie prowadzenia i aktualizowania dokumentacji dotyczącej ochrony danych osobowych u Administratora, w szczególności rejestru czynności przetwarzania;
i) poddawaniu, co najmniej raz w roku, przeglądowi Polityki Ochrony Danych Osobowych, pod kątem jej aktualności oraz zgodności deklarowanego w niej stanu z prawem;
j) nadzorowanie powierzania przetwarzania danych osobowych innym podmiotom, w szczególności nadzorowanie spełnienia wymagań rozporządzenia przez procesora;
k) nadzorowanie udostępniania danych osobowych;
l) inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych;
m) podejmowanie, wspólnie z Administratorem Danych oraz Administratorem Systemu Informatycznego, odpowiednich działań w przypadku naruszenia lub podejrzenia naruszenia bezpieczeństwa przetwarzania danych osobowych;
n) przygotowywaniu materiałów szkoleniowych z zakresu ochrony danych osobowych i prowadzeniu cyklicznych szkoleń osób upoważnianych do przetwarzania danych osobowych lub współpraca w tym zakresie z wyspecjalizowanym podmiotem zewnętrznym;
o) wyznaczanie w formie pisemnej, w porozumieniu z Administratorem Danych, swojego zastępcy na czas swojej nieobecności.

Nadto zobowiązuję się do:

1. sprawowania nadzoru nad prawidłowym stosowaniem się do zasad i procedur określonych w Polityce Ochrony Danych Osobowych oraz Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych;
2. udzielanie odpowiedzi na zapytania kierowane do Administratora Danych przez podmioty zewnętrzne, dotyczące przetwarzania danych osobowych u Administratora;
3. reprezentowanie Administratora oraz udział w czasie przeprowadzenia kontroli przez służby Prezesa Urzędu Ochrony Danych Osobowych;
4. prowadzenie i nadzorowanie korespondencji z Prezesem Urzędu Ochrony Danych Osobowych;
5. sprawowanie nadzoru nad nadawaniem uprawnień do przetwarzania danych osobowych w systemach informatycznych;
6. prowadzenie nadzoru nad fizycznym zabezpieczeniem obszarów przetwarzania danych osobowych;
7. sprawowanie nadzoru nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe;
8. sprawowanie nadzoru nad bezpieczeństwem danych osobowych zawartych na dyskach wymiennych, palmtopach, pamięciach przenośnych i innych nośnikach, a także w komputerach przenośnych;

9. sprawowanie nadzoru nad instalacjami i konfiguracjami oprogramowania systemowego, sieciowego;
10. sprawowanie nadzoru nad obiegiem oraz przechowywaniem dokumentacji zawierającej dane osobowe;
11. sprawowanie nadzoru nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników w systemach informatycznych Administratora oraz kontrolę dostępu do danych;
12. identyfikowanie i analizowanie zagrożeń oraz ryzyka, na które narażone mogą być dane osobowe przetwarzane u Administratora;
13. monitorowanie zabezpieczeń wdrożonych w celu ochrony danych osobowych;
14. przeprowadzanie kontroli w zakresie ochrony danych osobowych;
15. określanie potrzeb w zakresie zabezpieczenia danych osobowych;
16. podejmowanie odpowiednich działań w przypadkach naruszenia bezpieczeństwa danych;
17. nadzór nad prowadzeniem rejestru incydentów i zdarzeń wskazujących na naruszenie bezpieczeństwa danych osobowych;
18. dokonywanie modyfikacji i akceptacji proponowanych zmian, jak i okresowych kontroli polityk i procedur;
19. sprawowanie nadzoru nad procesem przyznawania praw dostępu;
20. organizowanie i prowadzenie szkoleń z zakresu ochrony danych osobowych;
21. opiniowanie zakupów w ramach Systemu Zarządzania Bezpieczeństwem Informacji;
22. opiniowanie wzorów dokumentów i umów;
23. nadzorowanie pracy Administratora Systemu Informatycznego;
24. nadzorowanie pracy osób upoważnionych do przetwarzania danych osobowych.

Naruszenie przez Inspektora Ochrony Danych obowiązków w zakresie wskazanym powyżej, może stanowić podstawę do podjęcia przez Administratora Danych przysługujących mu środków prawnych, a w szczególności może stanowić przyczynę uzasadniającą wypowiedzenie przez Administratora Danych umowy lub rozwiązanie tejże umowy bez wypowiedzenia, z winy naruszającego.

. . . . . .

(data i podpis Inspektora Ochrony Danych)

Przyjmuje oświadczenie

. . . . . .

(data i podpis osoby reprezentującej Administratora Danych)

	POLITYKA OCHRONA DANYCH OSOBOWYCH	Wersja	1.00
		Data opracowania	……...
		Właściciel	……...
ZGODY I KLAUZULE INFORMACYJNE – WZÓR			Załącznik nr 8

. . . . . .

(miejscowość, data)

Zgody przy pobieraniu danych

1. Klauzula zgody na przetwarzanie danych osobowych w rekrutacji
   Wyrażam zgodę na przetwarzanie moich ww. danych osobowych dla potrzeb rekrutacji na stanowisko *(Stanowisko pracy)* przez *(Nazwa administratora danych)*.
2. Klauzula zgody na przetwarzanie danych osobowych w przyszłych rekrutacjach
   Wyrażam zgodę na przetwarzanie moich ww. danych osobowych dla potrzeb przyszłych procesów rekrutacji przez *(Nazwa administratora danych)*.
3. Klauzula zgody na przetwarzanie danych osobowych celem publikacji w mediach
   Wyrażam zgodę na przetwarzanie moich danych osobowych w postaci *(Zakres danych)* w celu rozpowszechniania w mediach na następujących polach eksploatacji *(Pola eksploatacji)* przez *(Nazwa administratora danych)* zgodnie z ustawą z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (t.j. Dz.U. z 2017 r. poz. 880 ze zm.). Oświadczam, że zrzekam się dodatkowego wynagrodzenia z powyższego tytułu.
4. Klauzula zgody na przetwarzanie danych osobowych do celów marketingowych (DROGĄ ELEKTRONICZNĄ – MAILING)
   Wyrażam zgodę na przetwarzanie moich ww. danych osobowych, w celu prowadzenia marketingu bezpośredniego za pośrednictwem poczty elektronicznej przez *(Nazwa administratora danych)* zgodnie z ustawą z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (t.j. Dz.U. z 2017 r. poz. 1219).
5. Klauzula zgody na przetwarzanie danych osobowych do celów marketingowych (DROGĄ TELEFONICZNĄ – CALL CENTER)
   Wyrażam zgodę na przetwarzanie moich ww. danych osobowych, w celu prowadzenia marketingu bezpośredniego za pośrednictwem połączeń telefonicznych przez *(Nazwa administratora danych)* zgodnie z ustawą z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (t.j. Dz.U. z 2017 r. poz. 1907 ze zm.).
6. Klauzula wielokrotnej zgody na przetwarzanie danych osobowych z wieloma przykładowymi celami
   Zgodnie z art. 7 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. wyrażam zgodę na przetwarzanie ww. danych osobowych przez *(Nazwa administratora danych)* do celów:
   [ ] Przekazania innym podmiotom z grupy kapitałowej
   [ ] Przekazania podmiotom trzecim
   [ ] Uczestnictwa w promocji ……
   [ ] Uczestnictwa w konkursie ……

Klauzule informacyjne przy pobieraniu danych osobowych

1. Klauzula informacyjna przy pobieraniu danych bezpośrednio od osoby

   Zgodnie z art. 13 ust. 1 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. informuję, iż:

   1) Administratorem Pani/Pana danych osobowych jest *(Nazwa administratora danych)* z siedzibą w *(Adres administratora danych);*

   2) Inspektorem Ochrony Danych w *(Nazwa administratora danych)* jest Pan/Pani *(imię i nazwisko inspektora, e-mail lub inne dane kontaktowe);*

   3) Pani/Pana dane osobowe przetwarzane będą w celu *(Cel przetwarzania danych)* na podstawie *(należy podać podstawę prawną przetwarzania, np. art. 6 ust 1 pkt a/b/c/d/e/f. Przy podpunkcie f należy wskazać uzasadniony interes ADO lub strony trzeciej);*

   4) odbiorcą Pani/Pana danych osobowych będą *(należy wymienić kategorię odbiorców o ile istnieją);*

   5) Pani/Pana dane osobowe będą przekazywane do państwa trzeciego/organizacji międzynarodowej na podstawie: *(Należy podać podstawę prawną przekazania danych do państwa trzeciego).*

   6) Pani/Pana dane osobowe będą przechowywane przez okres *(jeżeli nie ma możliwości wskazania okresu przechowywania, należy podać kryterium ustalania tego okresu, np. do czasu wyłonienia zwycięzcy konkursu, do czasu zakończenia rekrutacji itd.);*

   7) Posiada Pani/Pan prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu, prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania (jeżeli przetwarzanie odbywa się na podstawie zgody), którego dokonano na podstawie zgody przed jej cofnięciem;

   8) ma Pani/Pan prawo wniesienia skargi do Prezesa Urzędu Ochrony danych osobowych, gdy uzna Pani/Pan, iż przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.;

   9) podanie przez Pana/Panią danych osobowych jest *(Należy podać np. wymogiem ustawowym/warunkiem umownym/warunkiem zawarcia umowy)*. Jest Pani/Pan zobowiązana/y do ich podania, a konsekwencją niepodania danych osobowych będzie *(Należy podać, jeżeli osoba, której dane dotyczą, jest zobowiązana do ich podania, należy wskazać ewentualne konsekwencje niepodania danych);*

10) Pani/Pana dane będą przetwarzane w sposób zautomatyzowany, w tym również w formie profilowania. Zautomatyzowane podejmowanie decyzji będzie odbywało się na zasadach *(Należy podać zasady profilowania)*, konsekwencją takiego przetwarzania będzie *(Należy wskazać istotne informacje o zasadach zautomatyzowanego podejmowania decyzji oraz informacje o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą. Np. w jaki sposób będą oceniane czynniki osobowe osoby fizycznej, natomiast przykładową konsekwencją takiego przetwarzania może być automatyczne odrzucenie elektronicznego wniosku kredytowego czy elektroniczne metody rekrutacji bez interwencji ludzkiej)*

2. Klauzula informacyjna przy pobieraniu danych niebezpośrednio od osoby
Zgodnie z art. 13 ust. 1 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. informuję, iż:

1) Administratorem Pani/Pana danych osobowych jest *(Nazwa administratora danych)* z siedzibą w *(Adres administratora danych);*

2) Inspektorem ochrony danych w *(Nazwa administratora danych)* jest Pan/Pani *(imię i nazwisko inspektora, e-mail lub inne dane kontaktowe);*

3) Pani/Pana dane osobowe przetwarzane będą w celu *(Cel przetwarzania danych) na podstawie (należy podać podstawę prawną przetwarzania np. art. 6 ust. 1 pkt a/b/c/d/e/f. Przy podpunkcie f należy wskazać uzasadniony interes ADO lub strony trzeciej);*

4) odbiorcą Pani/Pana danych osobowych będą *(należy wymienić kategorię odbiorców o ile istnieją);*

5) Pani/Pana dane osobowe będą przekazywane do państwa trzeciego/organizacji międzynarodowej na podstawie: *(Należy podać podstawę prawną przekazania danych do państwa trzeciego)*.

6) Pani/Pana dane osobowe będą przechowywane przez okres *(jeżeli nie ma możliwości wskazania okresu przechowywania należy podać kryterium ustalania tego okresu np. do czasu wyłonienia zwycięscy konkursu, do czasu zakończenia rekrutacji itd.);*

7) posiada Pani/Pan prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu, prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania (jeżeli przetwarzanie odbywa się na podstawie zgody), którego dokonano na podstawie zgody przed jej cofnięciem;

8) ma Pani/Pan prawo wniesienia skargi do Prezesa Urzędu ochrony Danych Osobowych, gdy uzna Pani/Pan, iż przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.;

9) Pani/Pana dane osobowe zostały pobrane z *(Należy podać źródło danych, również gdy dane zostały podane z publicznie dostępnego źródła)*

10) podanie przez Pana/Panią danych osobowych jest *(Należy podać np. wymogiem ustawowym/warunkiem umownym/warunkiem zawarcia umowy)*. Jest Pani/Pan zobowiązana/y do ich podania, a konsekwencją niepodania danych osobowych będzie *(Należy podać jeżeli osoba, której dane dotyczą, jest zobowiązana do ich podania, należy wskazać ewentualne konsekwencje niepodania danych);*

11) Pani/Pana dane będą przetwarzane w sposób zautomatyzowany, w tym również w formie profilowania. Zautomatyzowane podejmowanie decyzji będzie odbywało się na zasadach *(Należy podać zasady profilowania)*, konsekwencją takiego przetwarzania będzie *(Należy wskazać istotne informacje o zasadach zautomatyzowanego podejmowania decyzji oraz informacje o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą. Np. w jaki sposób będą oceniane czynniki osobowe osoby fizycznej, natomiast przykładową konsekwencją takiego przetwarzania może być automatyczne odrzucenie elektronicznego wniosku kredytowego czy elektroniczne metody rekrutacji bez interwencji ludzkiej)*.

. . . . . .

(data i podpis osoby reprezentującej

Administratora Danych)

. . . . . .

(data i podpis osoby upoważnionej)

* niepotrzebne skreślić

	POLITYKA OCHRONA DANYCH OSOBOWYCH	Wersja	1.00
		Data opracowania	……..
		Właściciel	……..
POLITYKA RETENCYJNA – WYKAZ OKRESÓW PRZECHOWYWANIA DANYCH – WZÓR			Załącznik nr 9

. . . . . .

(miejscowość, data)

Polityka retencyjna – Wykaz okresów przechowywania danych

Rodzaj danych osobowych	Podstawa ich przechowywania (Podstawa ustalenia okresu przechowywania)	Okres przechowywania danych
Akta osobowe pracowników	Od 25.05.2018 r. – art. 6 ust. 1 lit. b i c RODO, art. 9 ust. 2 lit. b) RODO Art. 22^1 w zw. z art. 94 ust. 9a Kodeksu pracy Art. 51u ustawy o narodowym zasobie archiwalnym i archiwach	10 lat od dnia zakończenia pracy u danego pracodawcy[607]
Dokumentacja płacowa (listy płac, karty wynagrodzeń, inne dowody, na podstawie których następuje ustalenie podstawy wymiaru emerytury lub renty)	Od 25.05.2018 r. – art. 6 ust. 1 lit. b i c RODO Art. 22^1 w zw. z art. 94 ust. 9a Kodeksu pracy Art. 125a ust. 4 ustawy o emeryturach i rentach z FUS Art. 51u ustawy o narodowym zasobie archiwalnym i archiwach	50 lat od dnia zakończenia pracy u płatnika 50 lat od dnia wytworzenia dokumentacji płacowej
Dane zakładowego funduszu świadczeń socjalnych	Od 25.05.2018 r. – art. 6 ust. 1 lit. b i c RODO Art. 22^1 w zw. z art. 94 ust. 9a kodeksu pracy Ustawa z dnia 4 marca 1994 roku o zakładowym funduszu socjalnym Art. 51u ustawy o narodowym zasobie archiwalnym i archiwach	50 lat od dnia zakończenia pracy u pracodawcy 50 lat od dnia wytworzenia dokumentacji płacowej
Oświadczenia pracowników dla celów obliczania miesięcznych zaliczek na podatek dochodowy od osób fizycznych	Od 25.05.2018 r. – art. 6 ust. 1 lit. b i c RODO Art. 31 ustawy z dnia 26 lipca 1991 r. o podatku dochodowym od osób fizycznych Rozporządzenie Ministra Finansów z dnia 23 listopada 2015 r. w sprawie określenia niektórych wzorów oświadczeń, deklaracji i informacji podatkowych obowiązujących w zakresie podatku dochodowego od osób fizycznych Art. 51u ustawy o narodowym zasobie archiwalnym i archiwach	50 lat od dnia zakończenia pracy u pracodawcy 50 lat od dnia wytworzenia dokumentacji płacowej
Zgłoszenia do ZUS	Od 25.05.2018 r. – art. 6 ust. 1 lit. b i c RODO Art. 36 ust. 8 ustawy o systemie ubezpieczeń społecznych	5 lat
Dokumentacja BHP	Od 25.05.2018 r. – art. 6 ust. 1 lit. b i c RODO Art. 237^4 Kodeksu pracy Rozporządzenie Ministra Gospodarki i Pracy z dnia 27 lipca 2004 r. w sprawie szkolenia w dziedzinie bezpieczeństwa i higieny pracy Rozporządzenie Rady Ministrów z dnia 1 lipca 2009 r. w sprawie ustalenia okoliczności i przyczyn wypadków przy pracy Art. 125a ust. 4 ustawy o emeryturach i rentach z FUS	50 lat od dnia zakończenia pracy u płatnika

[607] Z dniem 1 stycznia 2019 r. w życie weszła ustawa o zmianie niektórych ustaw w związku ze skróceniem okresu przechowywania akt pracowniczych oraz ich elektronizacją. Ustawa wprowadziła istotne zmiany dla pracodawców, którzy zostali zobowiązani do przechowywania akt pracowniczych przez 10 lat, a nie jak wcześniej – przez 50 lat. Ponadto, dokumentacja ta będzie mogła być prowadzona w formie elektronicznej. Aby skorzystać z krótszego okresu przechowywania akt w stosunku do pracowników zatrudnionych przed 1 stycznia 2019 roku, pracodawca został zobligowany do złożenia w ZUS raportu informacyjnego, w którym znajdą się informacje niezbędne do wyliczenia emerytury lub renty danego pracownika. W odniesieniu do pracowników zatrudnionych po 1 stycznia 2019 roku, okres przechowywania akt wynosi 10 lat, ale pracodawca został zobowiązany do wysyłania rozszerzonych miesięcznych raportów imiennych pracowników.

Ewidencja danych pracowników tymczasowych (wykonujących pracę na podstawie umowy o pracę oraz umowy prawa cywilnego)	Od 25.05.2018 r. – art. 6 ust. 1 lit. b i c RODO Art. 14a ustawy o zatrudnianiu pracowników tymczasowych	36 miesięcy od zakończenia prowadzenia ewidencji pracowników tymczasowych
Protokoły ustalenia okoliczności i przyczyn wypadku przy pracy, dokumentacja powypadkowa	Od 25.05.2018 r. – art. 6 ust. 1 lit. b i c RODO Art. 234 ust. 3^1 Kodeksu pracy	10 lat
Dokumenty aplikacyjne i dane kandydatów do pracy	Od 25.05.2018 r. – art. 6 ust. 1 lit. a i b RODO Art. 22^1 § 1 Kodeksu pracy	Do zakończenia procesu rekrutacji
Dokumentacja na potrzeby PFRON	Od 25.05.2018 r. – art. 6 ust. 1 lit. b i c RODO Ustawa o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych Art. 51u ustawy o narodowym zasobie archiwalnym i archiwach	50 lat od dnia zakończenia pracy u danego pracodawcy
Dane osobowe osób świadczących pracę na podstawie umów cywilnoprawnych, które zostały oskładkowane	Od 25.05.2018 r. – art. 6 ust. 1 lit. b i c RODO Art. 42 ust. 2 pkt 1) w zw. z art. 41 ust 1 ustawy o podatku dochodowym od osób fizycznych Art. 36 ust 2 w zw. z art. 9 w zw. z 6 ust. 1 pkt 4 w ustawy z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych	50 lat od zakończenia pracy ubezpieczonego u danego płatnika
Dane osobowe osób świadczących pracę na podstawie umów cywilnoprawnych, które nie zostały oskładkowane	Od 25.05.2018 r. – art. 6 ust. 1 lit. b i c RODO Brak regulacji ustawowej w zakresie okresu przetwarzania	Z uwagi na brak regulacji prawnych dotyczących okresu, przez jaki dane powinny być przetwarzane, decyzja w tym zakresie należy do administratora, stosownie do swoich potrzeb, przy czym należy zastrzec, że decyzja ta powinna być podjęta po przeprowadzeniu indywidulanej oceny każdego przypadku, z uwzględnieniem zasady celowości i minimalizacji danych. W przypadku, gdy cel przetwarzania danych został osiągnięty, dane powinny być trwale usunięte. wskazówką dotyczącą okresu przetwarzania danych może być okres przedawnienia tych roszczeń (np. umowa o dzieło, umowa zlecenia – 2 lata)
Prowadzenie strony internetowej Administratora	Od 25.05.2018 r. – art. 6 ust. 1 lit. b, c, f RODO	Z uwagi na brak regulacji prawnych dotyczących okresu, przez jaki dane powinny być przetwarzane, decyzja w tym zakresie należy do administratora, stosownie do swoich potrzeb, przy czym należy zastrzec, że decyzja ta powinna być podjęta po przeprowadzeniu indywidulanej oceny każdego przypadku, z uwzględnieniem zasady celowości i minimalizacji danych. W przypadku, gdy cel przetwarzania danych został osiągnięty, dane powinny być trwale usunięte. wskazówką dotyczącą okresu przetwarzania danych może być okres przedawnienia tych roszczeń (np. umowa o dzieło, umowa zlecenia – 2 lata)
Prowadzenie dokumentacji systemów informatycznych	Od 25.05.2018 r. – art. 6 ust. 1 lit. b, c, f RODO	Z uwagi na brak regulacji prawnych dotyczących okresu, przez jaki dane powinny być przetwarzane, decyzja w tym zakresie należy do administratora, stosownie do swoich potrzeb, przy czym należy zastrzec, że decyzja ta powinna być podjęta po przeprowadzeniu indywidulanej oceny każdego przypadku, z uwzględnieniem zasady celowości i minimalizacji danych. W przypadku, gdy cel przetwarzania danych został osiągnięty, dane powinny być trwale usunięte.
Realizacja projektów	Od 25.05.2018 r. – art. 6 ust. 1 lit. b, c, f RODO	Z uwagi na brak regulacji prawnych dotyczących okresu, przez jaki dane powinny być przetwarzane, decyzja w tym zakresie należy do administratora, stosownie do swoich potrzeb, przy czym należy zastrzec, że decyzja ta powinna być podjęta po przeprowadzeniu indywidulanej oceny każdego przypadku, z uwzględnieniem zasady celowości i minimalizacji danych. W przypadku, gdy cel przetwarzania danych został osiągnięty, dane powinny być trwale usunięte.
Prowadzenie szkoleń wewnętrznych	Od 25.05.2018 r. – art. 6 ust. 1 lit. b, c, f RODO	Z uwagi na brak regulacji prawnych dotyczących okresu, przez jaki dane powinny być przetwarzane, decyzja w tym zakresie należy do administratora, stosownie do swoich potrzeb, przy czym należy zastrzec, że decyzja ta powinna być podjęta po przeprowadzeniu indywidulanej oceny każdego przypadku, z uwzględnieniem zasady celowości i minimalizacji danych. W przypadku, gdy cel przetwarzania danych został osiągnięty, dane powinny być trwale usunięte.

Prowadzenie wykazu pracowników w związku ze sprawami obronnymi, militaryzacyjnymi i mobilizacyjnymi	Art. 6 ust. 1 lit. b), c) i f) RODO Ustawa z dnia 16 listopada 2016r. o zmianie ustawy o powszechnym obowiązku obrony Rzeczypospolitej Polskiej oraz niektórych innych ustaw (Dz.U. z 2016r., poz. 2138) Rozporządzenie Rady Ministrów z dnia 13 stycznia 2004r. w sprawie ogólnych zasad wykonywania zadań w ramach powszechnego obowiązku obrony (Dz.U. z 2004r., Nr 16, poz. 152) Rozporządzenie Rady Ministrów z dnia 21 września 2004 r. w sprawie reklamowania od obowiązku pełnienia czynnej służby wojskowej w razie ogłoszenia mobilizacji i w czasie wojny (Dz.U. z 2004r., Nr 210, poz. 2136) Rozporządzenie Rady Ministrów z dnia 24 listopada 2009 r. w sprawie militaryzacji jednostek organizacyjnych wykonujących zadania na rzecz obronności lub bezpieczeństwa państwa (Dz.U. z 2009r., Nr 210, poz. 1612) Rozporządzenie Rady Ministrów z dnia 24 czerwca 2003 r. z sprawie obiektów szczególnie ważnych dla bezpieczeństwa i obronności państwa oraz ich szczególnej ochrony	Z uwagi na brak regulacji prawnych dotyczących okresu, przez jaki dane powinny być przetwarzane, decyzja w tym zakresie należy do administratora, stosownie do swoich potrzeb, przy czym należy zastrzec, że decyzja ta powinna być podjęta po przeprowadzeniu indywidulanej oceny każdego przypadku, z uwzględnieniem zasady celowości i minimalizacji danych. W przypadku, gdy cel przetwarzania danych został osiągnięty, dane powinny być trwale usunięte.
Prowadzenie wykazu osób upoważnionych do informacji niejawnych, oraz osób którym odmówiono wydania poświadczenia bezpieczeństwa lub je cofnięto	Art. 6 ust. 1 lit. b), c) i f) RODO oraz art. 10 RODO Ustawa o ochronie informacji niejawnych oraz przepisy wykonawcze do niej	20 lat o zakończenia postępowania zwykłego sprawdzającego o udzielenia poświadczenia bezpieczeństwa
Prowadzenie korespondencji mailowej wewnętrznej i zewnętrznej	Art. 6 ust. 1 lit. b), c) i f) RODO	Z uwagi na brak regulacji prawnych dotyczących okresu, przez jaki dane powinny być przetwarzane, decyzja w tym zakresie należy do administratora, stosownie do swoich potrzeb, przy czym należy zastrzec, że decyzja ta powinna być podjęta po przeprowadzeniu indywidulanej oceny każdego przypadku, z uwzględnieniem zasady celowości i minimalizacji danych. W przypadku, gdy cel przetwarzania danych został osiągnięty, dane powinny być trwale usunięte.
Prowadzenie ewidencji delegacji i wyjazdów służbowych	Art. 6 ust. 1 lit. b), c) i f) RODO	Z uwagi na brak regulacji prawnych dotyczących okresu, przez jaki dane powinny być przetwarzane, decyzja w tym zakresie należy do administratora, stosownie do swoich potrzeb, przy czym należy zastrzec, że decyzja ta powinna być podjęta po przeprowadzeniu indywidulanej oceny każdego przypadku, z uwzględnieniem zasady celowości i minimalizacji danych. W przypadku, gdy cel przetwarzania danych został osiągnięty, dane powinny być trwale usunięte.
Dane klientów/kontrahentów zawarte w dokumentacji finansowo-księgowej	Od 25.05.2018 r. – art. 6 ust. 1 lit. c RODO Art. 32 ust. 1, art. 86 ust. 1 , art. 88 ust. 1 Ordynacji podatkowej Art. 74 ustawy o rachunkowości	5 lat, jednak nie krócej niż do czasu upływu okresu przedawnienia zobowiązania podatkowego
Monitoring	Od 25.05.2018 r. – art. 6 ust. 1 lit. f RODO Brak regulacji ustawowej w zakresie okresu przetwarzania	Z uwagi na brak regulacji prawnych dotyczących okresu, przez jaki dane powinny być przetwarzane, decyzja w tym zakresie należy do administratora, stosownie do swoich potrzeb, przy czym należy zastrzec, że decyzja ta powinna być podjęta po przeprowadzeniu indywidulanej oceny każdego przypadku, z uwzględnieniem zasady celowości i minimalizacji danych. W przypadku, gdy cel przetwarzania danych został osiągnięty, dane powinny być trwale usunięte. W krajach UE zwykle przyjmuje się, że nagrania z monitoringu powinny być przechowywane przez okres do 30 dni.
Dane osobowe klientów	Od 25.05.2018 r. – art. 6 ust. 1 lit. b, c i f RODO oraz art. 10 RODO Brak regulacji ustawowej w zakresie okresu przetwarzania	Z uwagi na brak regulacji prawnych dotyczących okresu, przez jaki dane powinny być przetwarzane, decyzja w tym zakresie należy do administratora, stosownie do swoich potrzeb, przy czym należy zastrzec, że decyzja ta powinna być podjęta po przeprowadzeniu indywidulanej oceny każdego przypadku, z uwzględnieniem zasady celowości i minimalizacji danych. W przypadku, gdy cel przetwarzania danych został osiągnięty, dane powinny być trwale usunięte. Wskazówką dotyczącą okresu przetwarzania danych może być okres przedawnienia tych roszczeń.
Dane osobowe kontrahentów	Od 25.05.2018 r. – art. 6 ust. 1 lit. b i f RODO Brak regulacji ustawowej w zakresie okresu przetwarzania	Z uwagi na brak regulacji prawnych dotyczących okresu, przez jaki dane powinny być przetwarzane, decyzja w tym zakresie należy do administratora, stosownie do swoich potrzeb, przy czym należy zastrzec, że decyzja ta powinna być podjęta po przeprowadzeniu indywidulanej oceny każdego przypadku, z uwzględnieniem zasady celowości i minimalizacji danych. W przypadku, gdy cel przetwarzania danych został osiągnięty, dane powinny być trwale usunięte. Wskazówką dotyczącą okresu przetwarzania danych może być okres przedawnienia tych roszczeń.
Książka korespondencji	Od 25.05.2018 r. – art. 6 ust. 1 lit. f RODO Brak regulacji ustawowej w zakresie okresu przetwarzania	Z uwagi na brak regulacji prawnych dotyczących okresu, przez jaki dane powinny być przetwarzane, decyzja w tym zakresie należy do administratora, stosownie do swoich potrzeb, przy czym należy zastrzec, że decyzja ta powinna być podjęta po przeprowadzeniu indywidulanej oceny każdego przypadku, z uwzględnieniem zasady celowości i minimalizacji danych. W przypadku, gdy cel przetwarzania danych został osiągnięty, dane powinny być trwale usunięte.

Księga gości	Od 25.05.2018 r. – art. 6 ust. 1 lit. f RODO Brak regulacji ustawowej w zakresie okresu przetwarzania	Z uwagi na brak regulacji prawnych dotyczących okresu, przez jaki dane powinny być przetwarzane, decyzja w tym zakresie należy do administratora, stosownie do swoich potrzeb, przy czym należy zastrzec, że decyzja ta powinna być podjęta po przeprowadzeniu indywidulanej oceny każdego przypadku, z uwzględnieniem zasady celowości i minimalizacji danych. W przypadku, gdy cel przetwarzania danych został osiągnięty, dane powinny być trwale usunięte..
Księga wejść i wyjść	Od 25.05.2018 r. – art. 6 ust. 1 lit. f RODO Brak regulacji ustawowej w zakresie okresu przetwarzania	Z uwagi na brak regulacji prawnych dotyczących okresu, przez jaki dane powinny być przetwarzane, decyzja w tym zakresie należy do administratora, stosownie do swoich potrzeb, przy czym należy zastrzec, że decyzja ta powinna być podjęta po przeprowadzeniu indywidulanej oceny każdego przypadku, z uwzględnieniem zasady celowości i minimalizacji danych. W przypadku, gdy cel przetwarzania danych został osiągnięty, dane powinny być trwale usunięte.
Dane osobowe uczestników postępowań przedsądowych, sądowych, administracyjnych, których stroną jest administrator, w tym dłużników administratora	Od 25.05.2018 r. – art. 6 ust. 1 lit. c i f RODO oraz art. 10 RODO Brak regulacji ustawowej w zakresie okresu przetwarzania	Z uwagi na brak regulacji prawnych dotyczących okresu, przez jaki dane powinny być przetwarzane, decyzja w tym zakresie należy do administratora, stosownie do swoich potrzeb, przy czym należy zastrzec, że decyzja ta powinna być podjęta po przeprowadzeniu indywidulanej oceny każdego przypadku, z uwzględnieniem zasady celowości i minimalizacji danych. W przypadku, gdy cel przetwarzania danych został osiągnięty, dane powinny być trwale usunięte.
Dane osobowe uczestników postępowań przedsądowych, sądowych, administracyjnych, innych niż klienci	Od 25.05.2018 r. – art. 6 ust. 1 lit. c i f RODO oraz art. 10 RODO Brak regulacji ustawowej w zakresie okresu przetwarzania	Z uwagi na brak regulacji prawnych dotyczących okresu, przez jaki dane powinny być przetwarzane, decyzja w tym zakresie należy do administratora, stosownie do swoich potrzeb, przy czym należy zastrzec, że decyzja ta powinna być podjęta po przeprowadzeniu indywidulanej oceny każdego przypadku, z uwzględnieniem zasady celowości i minimalizacji danych. W przypadku, gdy cel przetwarzania danych został osiągnięty, dane powinny być trwale usunięte.
Dane pełnomocników stron postępowania	Od 25.05.2018 r. – art. 6 ust. 1 lit. c i f RODO oraz art. 10 RODO Brak regulacji ustawowej w zakresie okresu przetwarzania	Z uwagi na brak regulacji prawnych dotyczących okresu, przez jaki dane powinny być przetwarzane, decyzja w tym zakresie należy do administratora, stosownie do swoich potrzeb, przy czym należy zastrzec, że decyzja ta powinna być podjęta po przeprowadzeniu indywidulanej oceny każdego przypadku, z uwzględnieniem zasady celowości i minimalizacji danych. W przypadku, gdy cel przetwarzania danych został osiągnięty, dane powinny być trwale usunięte.
Prowadzenie postępowań przetargowych/ ofertowych/ o zamówienie	Od 25.05.2018 r. – art. 6 ust. 1 lit. c i f RODO oraz art. 10 RODO Prawo zamówień publicznych (Pzp)	Zamawiający – w ramach postępowania o udzielnie zamówienia publicznego, powinien przechowywać protokół wraz z załącznikami przez okres 4 lat od dnia zakończenia postępowania o udzielenie zamówienia w sposób gwarantujący jego nienaruszalność. Zgodnie z definicją legalną postępowanie kończy się z momentem dokonania wyboru oferty wykonawcy, z którym zostanie zawarta umowa w sprawie zamówienia publicznego, lub – w przypadku zamówienia z wolnej ręki – wynegocjowania postanowień takiej umowy. Odstępstwo od konieczności przechowywania pewnych dokumentów dotyczy zwrotów dokumentów wykonawcom, których oferty nie zostały wybrane , na ich wniosek złożone przez nich: plany, projekty, rysunki, modele, próbki wzory, programy komputerowe oraz inne podobne materiały. W przypadku zamówień, ofert, przetargów prowadzonych poza trybem ustawy Prawo zamówień publicznych z uwagi na brak regulacji prawnych dotyczących okresu, przez jaki dane powinny być przetwarzane, decyzja w tym zakresie należy do administratora, stosownie do swoich potrzeb, przy czym należy zastrzec, że decyzja ta powinna być podjęta po przeprowadzeniu indywidulanej oceny każdego przypadku, z uwzględnieniem zasady celowości i minimalizacji danych. W przypadku, gdy cel przetwarzania danych został osiągnięty, dane powinny być trwale usunięte. wskazówką dotyczącą okresu przetwarzania danych może być okres przedawnienia tych roszczeń.

Dane związane z nieruchomościami Administratora	Od 25.05.2018 r. – art. 6 ust. 1 lit. b, c i f RODO oraz art. 10 RODO Ustawa Prawo budowlane	Zgodnie ustawą Prawo budowlane właściciel (zarządca) budynku jest obowiązany przechowywać przez okres istnienia budynku dokumentację budowy, tj. pozwolenia na budowę wraz z projektem budowalnym, decyzje zatwierdzające zmiany w projekcie, decyzję o pozwoleniu na użytkowanie, dziennik budowy, protokoły odbiorów częściowych i końcowych, a w miarę potrzeby także rysunki i opisy służące realizacji obiektu, operaty geodezyjne i książkę obmiarów. Ustawa nakazuje także gromadzić dokumentację powykonawczą, czyli dokumentację budowy z naniesionymi zmianami dokonanymi w toku wykonywania robót. Właściciel powinien także przechowywać przekazane mu przez inwestora instrukcje obsługi i eksploatacji instalacji i urządzeń związanych z budynkiem. Ponadto ma obowiązek gromadzić dokumenty tworzone w okresie wykorzystywania budynku, w tym książki obiektu budowlanego, w której ujawnia się zapisy o badaniach i kontrolach stanu technicznego oraz o remontach i przebudowach budynku w czasie jego użytkowania. W pozostałym zakresie, w szczególności KW nieruchomości, umowy itp., decyzja w zakresie przechowywania danych należy do administratora, stosownie do swoich potrzeb, przy czym należy zastrzec, że decyzja ta powinna być podjęta po przeprowadzeniu indywidulanej oceny każdego przypadku, z uwzględnieniem zasady celowości i minimalizacji danych. W przypadku, gdy cel przetwarzania danych został osiągnięty, dane powinny być trwale usunięte. Wskazówką dotyczącą okresu przetwarzania danych może być okres przedawnienia tych roszczeń, jednakże okres przedawnienia nie powinien być traktowany jako stały wyznacznik okresu przechowywania danych.
Dane uczestników konferencji	Od 25.05.2018 r. – art. 6 ust. 1 lit. b, c i f RODO Brak regulacji ustawowej w zakresie okresu przetwarzania	Z uwagi na brak regulacji prawnych dotyczących okresu, przez jaki dane powinny być przetwarzane, decyzja w tym zakresie należy do administratora, stosownie do swoich potrzeb, przy czym należy zastrzec, że decyzja ta powinna być podjęta po przeprowadzeniu indywidulanej oceny każdego przypadku, z uwzględnieniem zasady celowości i minimalizacji danych. W przypadku, gdy cel przetwarzania danych został osiągnięty, dane powinny być trwale usunięte.
Rejestr skarg i wniosków	Od 25.05.2018 r. – art. 6 ust. 1 lit. b, c i f RODO Brak regulacji ustawowej w zakresie okresu przetwarzania	Z uwagi na brak regulacji prawnych dotyczących okresu, przez jaki dane powinny być przetwarzane, decyzja w tym zakresie należy do administratora, stosownie do swoich potrzeb, przy czym należy zastrzec, że decyzja ta powinna być podjęta po przeprowadzeniu indywidulanej oceny każdego przypadku, z uwzględnieniem zasady celowości i minimalizacji danych. W przypadku, gdy cel przetwarzania danych został osiągnięty, dane powinny być trwale usunięte.

. . . . . .

(data i podpis osoby reprezentującej

Administratora Danych)

Potwierdzam

. . . . . .

(data i podpis Inspektora Ochrony Danych)

	POLITYKA OCHRONA DANYCH OSOBOWYCH	Wersja	1.00
		Data opracowania	……..
		Właściciel	……..
OPIS ZABEZPIECZEŃ FIZYCZNYCH, TECHNICZNYCH I PROGRAMOWYCH – WZÓR			Załącznik nr 10

. . . . . .

(miejscowość, data)

Opis zabezpieczeń ochrony fizycznej danych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

Lp.	Środek ochrony technicznej i fizycznej	Środek ochrony organizacyjnej	Uwagi
1.	Dane osobowe przechowywane są w pomieszczeniu zabezpieczonym drzwiami zwykłymi (niewzmacnianymi, nie przeciwpożarowymi)	Do przetwarzania danych osobowych dopuszczono wyłącznie osoby posiadające upoważnienie nadane przez Administratora Danych	
2.	Dane osobowe przechowywany jest w pomieszczeniu, w którym okna zabezpieczone są za pomocą krat, rolet lub folii antywłamaniowej	Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych	
3.	Pomieszczenia, w którym przetwarzany jest zbiór danych osobowych wyposażone są w system alarmowy przeciwwłamaniowy	Wyznaczono Inspektora Ochrony Danych	
4.	Dostęp do pomieszczeń, w których przetwarzane są dane osobowe objęte są systemem kontroli dostępu (pomieszczenia są zamykane na klucze, które wydawane są na podstawie pisemnych upoważnień i których pobranie odnotowane jest w rejestrze)	Wyznaczono Administratora Systemu Informatycznego	
5.	Dostęp do pomieszczeń, w których przetwarzane są dane osobowe kontrolowany jest przez system monitoringu z zastosowaniem kamer przemysłowych	Opracowano i wdrożono Politykę Ochrony Danych Osobowych	
6.	Dostęp do pomieszczeń, w których przetwarzane są dane osobowe jest w czasie nieobecności zatrudnionych tam pracowników nadzorowany przez służbę ochrony	Opracowano i wdrożono Instrukcję Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych	
7.	Dostęp do pomieszczeń, w których przetwarzane są dane osobowe przez cała dobę jest nadzorowany przez służbę ochrony		
8.	Dane osobowe w formie papierowej przechowywane jest w zamkniętej niemetalowej szafie	Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych	
9.	Dane osobowe w formie papierowej przechowywany jest w zamkniętej metalowej szafie	Przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego	
10.	Dane osobowe w formie papierowej przechowywane są w zamkniętym sejfie lub kasie pancernej	Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania tajemnicy danych osobowych	
11.	Kopie zapasowe/archiwalne danych osobowych przechowywane są w zamkniętej niemetalowej szafie	Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym	
12.	Kopie zapasowe/archiwalne danych osobowych przechowywane są w zamkniętej metalowej szafie.	Kopie zapasowe zbioru danych osobowych przechowywane są w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco	
13.	Pomieszczenie, w którym przetwarzane są dane osobowe zabezpieczone jest przed skutkami pożaru za pomocą systemu przeciwpożarowego i/lub wolnostojącej gaśnicy usytuowanej w ciągu komunikacyjnym		
14.	Dokumenty/nośniki danych zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów, sporządzany jest protokół zniszczenia.		

Opis zabezpieczeń sprzętowych infrastruktury informatycznej i telekomunikacyjnej dla fizycznych elementów systemu teleinformatycznego

Lp.	Środek ochrony sprzętowej	Środek ochrony organizacyjnej	Uwagi
1.	Elementy infrastruktury teleinformatycznej umieszczone są w pomieszczeniach: ▪ serwerowych – serwery, aktywne urządzenia sieciowe, urządzenia pamięci masowych – pomieszczania wydzielone, zabezpieczone przez system kontroli dostępu; ▪ pomieszczeniach pracy – stacje końcowe stacjonarne i mobilne – pomieszczona zabezpieczone drzwiami z zamkami.	Dostęp do pomieszczeń serwerowych ograniczony do wydzielonej grupy administratorów. Dostęp innych osób (serwisu, obsługi technicznej) odbywa się pod nadzorem osób upoważnionych. Pomieszczenia ogólne kontrolowane są strefowo przez system kontroli dostępu i dostęp do nich mają tylko pracownicy Spółki, poza obszarem dostępnym dla gości (nadzór nad gośćmi sprawują opiekunowie)	
2.	Klaster firewall – ochrona styku sieci lokalnej z siecią globalną, kontrola ruchu wychodzący i przychodzący.	Zdefiniowane są filtry treści oraz czarne listy serwisów niedostępnych z sieci, ustawione są parametry reputacji serwisów internetowych.	
3.	Firewall wewnętrzny – wydzielenie stref dla określonych systemów		
4.	System zabezpieczenia infrastruktury poczty internetowej – system zabezpieczenia antyspam oraz antywirus	Zdefiniowane są parametry reputacji serwerów pocztowych, ustawione polityki antywirusowe.	
5.	System zabezpieczenia mobilnych stacji roboczych – szyfrowanie nośników wewnętrznych		

Opis zabezpieczeń technicznych i programowych dla procedur, aplikacji, programów, baz danych i innych narzędzi

	System stacji końcowych		
	Środek ochrony technicznej i programowej	**Środek ochrony organizacyjnej**	**Uwagi**
1.	Dostęp do stacji roboczej zabezpieczony jest hasłem. Wszyskie stacje robocze pracują w domenie ActiveDirectory i dostęp do ich zasobów wymaga autoryzacji.	Określone są polityki dotyczące długości, czasu obowiązywania i złożoności haseł dostępowych.	
2.	Stacje robocze mobilne mają dyski szyfrowane, system szyfrowania jest centralnie zarządzany.	Określone są zasady, które i w jakim zakresie stacje mobilne mają szyfrowane dyski.	
3.	Zasoby stacji roboczych są zabezpieczone poprzez ustawienie odpowiednich polis, które umożliwiają użytkownikowi dostęp tylko do określonych zasobów.	Wyznaczeni administratorzy systemu AD kontrolują aktualność polis na stacjach roboczych, aktualizują je w przypadku zmiany zasad obowiązujących w Spółce.	
4.	Zdefiniowane są różne poziomy dostępu do stacji: administrator (użytkownik uprzywilejowany), użytkownik zaawansowany (posiada możliwość włączania określonych funkcji systemowych, nie może dokonywać zmian w uprawnieniach), użytkownik stacji roboczej (standardowy użytkownik posiadający dostęp tylko do swoich zasobów)	Wyznaczeni są administratorzy AD oraz każdy z nich posiada indywidualne konto administratora umożliwiające identyfikacje w logach systemowych. Określone są dla każdego administratora poziomy uprawnień	
5.	Dane szczególnie ważne oraz wrażliwe są archiwizowane na zasobach sieciowych (dyskach sieciowych lub w systemie wersjonowania dokumentów – SNV).	Każda komórka posiada dostęp do zasobu sieciowego, zdefiniowane są odpowiednie uprawnienia do poszczególnych zasobów (katalogów).	
6.	Stacje robocze zabezpieczone są systemem antywirusowym zarządzanym centralnie oraz podłączone są do centralnego systemu aktualizacji. Zarządzanie aktualizacjami jest scentralizowane.	Zdefiniowana jest polityka częstotliwości aktualizacji zabezpieczeń antywirusowych oraz aktualizacji systemów i aplikacji.	
	System urządzeń sieciowych		
1.	Dostęp do urządzeń sieciowych jest chroniony hasłem. Wszystkie urządzenia sieciowe wymagają autoryzacji nazwą użytkownika i hasłem, system kont i haseł jest zarządzany centralnie.	Wyznaczeni są administratorzy urządzeń sieciowych, każdy administrator ma indywidualne konto umożliwiające identyfikację wykonywanych zmian.	
2.	Dostęp do konsoli każdego urządzenia sieciowego jest zabezpieczony hasłem, urządzenia zainstalowane są w pomieszczeniach chronionych przez system kontroli dostępu.	Wyznaczeni administratorzy mają dostęp do pomieszczeń serwerowni i możliwość podłączenia się fizycznie do urządzeń. Dostęp do serwerowni i dostęp do urządzeń jest monitorowany.	
3.	Zmiany konfiguracji urządzeń sieciowych są monitorowane i logowane. Prowadzony jest system zarządzania zmianami konfiguracji.	System zarządzania konfiguracją informuje administratorów o każdej zmianie konfiguracji, wyznaczony administrator monitoruje wszystkie zmiany.	
4.	Zarządzanie urządzeniami sieciowymi odbywa się w wydzielonym segmencie sieci (w VLANie administracyjnym)		
5.	Urządzenia sieciowe są monitorowane poprzez narzędzie Observium. W narzędziu przechowywane są logi oraz konfiguracje urządzeń.		
	System serwerów aplikacyjnych		
1.	Dostęp serwerów aplikacyjnych chroniony jest systemem haseł. Wyróżnione są różne poziomy dostępu , zależne od poziomu administratora/użytkownika. Wyróżniamy następujące poziomy dostępu: administrator systemu (użytkownik uprzywilejowany z pełnym dostępem do systemu serwera), administrator aplikacji (użytkownik uprzywilejowany z pełnym dostępem do określonej, zarządzanej przez niego aplikacji), użytkownik zaawansowany (użytkownik posiadający dostępy do dodatkowych zasobów serwera) oraz użytkownik.	Wyznaczeni są administratorzy poszczególnych systemów i przydzielone są im indywidualne konta dostępowe. Zdefiniowane są również inne role w systemach tj. właściciela informacyjnego, administratora aplikacji itd.	

System stacji końcowych			
	Środek ochrony technicznej i programowej	**Środek ochrony organizacyjnej**	**Uwagi**
2.	Dostęp do aplikacji jest chroniony niezależnym od systemu stacji końcowych i serwerów systemem haseł i ról w aplikacji. Wprowadzone są dodatkowe role ograniczające dostęp do zasobów informacyjnych użytkowanych aplikacji.	Określone są polityki dotyczące długości, czasu obowiązywania i złożoności haseł dostępowych.	
3.	Aplikacje zarządzające serwerami instalowane są na określonych, ściśle wytypowanych stacjach roboczych administratorów.	Wyznaczone są stacje robocze na których zainstalowane są panele administracyjne serwerów aplikacyjnych.	
4.	Wszystkie serwery aplikacyjne i bazodanowe są umieszczone w wydzielonym segmencie sieciowym, chronionym poprzez dodatkowe listy dostępowe zdefiniowane na urządzeniach sieciowych.		
5.	Serwery zabezpieczone są systemem ochrony antywirusowej oraz dostęp do nich jest chroniony poprzez firewalle programowe serwerów.	Zdefiniowana jest polityka częstotliwości aktualizacji zabezpieczeń antywirusowych oraz aktualizacji systemów i aplikacji.	
6.	Operacje dokonywane przez administratorów i użytkowników serwerów są logowane, a logi systemu są archiwizowane.	Zdefiniowana jest polityka archiwizacji logów i długość ich przechowywania. Zdefiniowany jest zakres informacyjny logów systemowych.	
7.	Zasoby serwerów są archiwizowane, kopie zapasowe przechowywane są na wydzielonych dyskach (poza archiwizowanymi serwerami) oraz na nośnikach zewnętrznych przechowywanych poza serwerowniami.	Zdefiniowana jest polityka archiwizacji systemów i długość ich przechowywania. Zdefiniowany jest zakres informacyjny archiwizacji systemów.	
System aplikacji oraz baz danych			
1.	Dostęp do aplikacji i baz danych chroniony jest hasłami (system jest niezależny od systemu haseł dostępowych do stacji roboczych).	Określone są polityki dotyczące długości, czasu obowiązywania i złożoności haseł dostępowych.	
2.	W aplikacjach oraz bazach danych zdefiniowane są różne poziomy dostępu do danych. Wydzielone są następujące konta: administrator aplikacji, administrator bazy danych, użytkownik aplikacji – bazy danych.	Wyznaczeni są administratorzy poszczególnych systemów i przydzielone są im indywidualne konta dostępowe. Zdefiniowane są również inne role w systemach tj. właściciela informacyjnego, administratora aplikacji itd.	
3.	Bazy danych są centralnie archiwizowane, kopie zapasowe są przechowywane poza serwerowniami.	Zdefiniowana jest polityka archiwizacji systemów i długość ich przechowywania. Zdefiniowany jest zakres informacyjny archiwizacji systemów.	
4.	Operacje dotyczące aplikacji i baz danych wykonywane przez administratorów i użytkowników uprzywilejowanych są logowane, a logi systemowe są archiwizowane.	Zdefiniowana jest polityka archiwizacji logów i długość ich przechowywania. Zdefiniowany jest zakres informacyjny logów systemowych.	
5.	Dostęp administratorski do aplikacji i baz danych możliwy jest tylko z określonych segmentów sieci.		
System poczty, styku sieci firmowej z siecią INTERNET, strony WWW			
1.	Dostęp do poczty odbywa się tylko i wyłącznie przy wykorzystaniu łącza szyfrowanego (protokół https) oraz wymaga identyfikacji nazwą użytkownika i hasłem.	Określone są polityki dotyczące długości, czasu obowiązywania i złożoności haseł dostępowych.	
2.	System poczty jest zabezpieczony poprzez moduł antyspam oraz moduł antywirusowy z automatyczna funkcją aktualizacji sygnatur oraz reputacji serwerów.	Zdefiniowana jest polityka utrzymywania wsparcia producenta dla systemów: antyspamowego oraz antywirusowego.	
3.	System ochrony styku sieci firmowej z siecią INTERNET jest automatycznie uaktualniamy, posiada automatycznie uaktualnienie reputacje serwerów oraz kategorie blokowanych stron.	Zdefiniowana jest polityka utrzymywania wsparcia producenta dla systemu zabezpieczenia styku sieci firmowej z siecią INTERNET	
4.	System poczty i styku sieci loguje wszystkie dostępy do sieci i zasobów serwera pocztowego z sieci wewnętrznej i zewnętrznej.	Zdefiniowana jest polityka archiwizacji logów i długość ich przechowywania. Zdefiniowany jest zakres informacyjny logów systemowych.	
5.	Dostęp administratorów do systemu jest zabezpieczony hasłem i jest możliwy z określonych segmentów sieci.	Wyznaczeni są administratorzy poszczególnych systemów i przydzielone są im indywidualne konta dostępowe. Zdefiniowane są również inne role w systemach.	
System kadrowo-finansowy oraz system kontroli dostępu i rozliczania czasu pracy			
1.	Dostęp do systemów jest chroniony dodatkowymi hasłami, unikalnymi dla każdego systemu niezależnymi od kont dostępowych do stacji roboczych.	Określone są polityki dotyczące długości, czasu obowiązywania i złożoności haseł dostępowych.	
2.	Zestaw pól informacyjnych dostępnych w aplikacjach jest uzależniony od posiadanych uprawnień, jest definiowany przez administratora/ właściciela informacji.	Wyznaczeni są administratorzy poszczególnych systemów i przydzielone są im indywidualne konta dostępowe. Zdefiniowane są również inne role w systemach.	
3.	Dostęp serwisowy do systemu kadrowo-finansowego (Xpertis) odbywa się na terenie Spółki przy uprawnionym pracowniku. Dostęp jest możliwy z wydzielonej do tego celu stacji roboczej.	Podpisane są odpowiednie umowy dotyczące dostępu do danych przez firmę serwisującą system.	
4.	Dostęp serwisowy do systemu kontroli dostępu i rozliczania czasu pracy odbywa się poprzez kanał zdalny, zabezpieczony szyfrowanym łączem (VPN) z tokenen sprzętowym. Dostęp jest udzielany tylko do maszyny wirtualnej systemu i monitorowany jest w logach systemowych.	Podpisane są odpowiednie umowy dotyczące dostępu do danych przez firmę serwisującą system. Okna serwisowe są otwierane tylko na czas konieczny do serwisowania systemu. Po zakończeniu obsługi serwisowej dostęp do systemu jest zamknięty dla firmy serwisującej.	

. . . . . .

(data i podpis osoby reprezentującej

Administratora Danych)

	POLITYKA OCHRONA DANYCH OSOBOWYCH	**Wersja**	1.00
		Data opracowania	……...
		Właściciel	……...
REJESTR PROCESORÓW – WZÓR			Załącznik nr 11

. . . . . .

(miejscowość, data)

Rejestr podmiotów zewnętrznych, którym powierzono przetwarzanie danych (procesorów)

L.p.	Nazwa podmiotu, z którym zawarto umowę powierzenia	Data powierzenia	Cel powierzenia	Zakres powierzonych danych
1.	*(należy wskazać konkretne dane identyfikujące podmiot, z którym zawarto umowę powierzenia)*		*(np. realizowanie wsparcia technicznego w zakresie prawidłowego działania systemu informatycznego użytkowanego przez spółkę)*	*(należy wskazać lub opisać, do jakich konkretnie danych procesor może mieć dostęp na podstawie umowy powierzenia – wszelkie informacje które przetwarzane są w formie elektronicznej, w zakresie niezbędnym do dokonania konkretnej czynności wynikającej z umowy)*
2.				
3.				
4.				

ADMINISTRATOR DANYCH:

……

(data i podpis)

	POLITYKA OCHRONA DANYCH OSOBOWYCH	Wersja	1.00
		Data opracowania	……...
		Właściciel	……...
PROTOKÓŁ Z CZYNNOŚCI AUDYTOWYCH – WZÓR			Załącznik nr 12

. . . . . .

(miejscowość, data)

Protokół z czynności audytowych doraźnych w zakresie danych osobowych

1. Nazwa kontrolowanej komórki organizacyjnej:. . . . . .
2. Procesy na danych osobowych, których przetwarzanie podlega kontroli:

   . . . . . .

   . . . . . .

   . . . . . .
3. Data wykonania czynności audytowych doraźnych:. . . . . .
4. Imię i nazwisko (imiona i nazwiska) oraz stanowisko osoby/osób wykonującej/ych czynności audytowych:

   . . . . . .

   . . . . . .

   . . . . . .
5. Imiona i nazwiska osób udzielających informacji dotyczących ochrony danych osobowych w audytowanej komórce organizacyjnej: . . . . . .
6. Czynności dokonane:. . . . . .

   . . . . . .

   . . . . . .

   . . . . . .
7. Ustalenia dokonane w trakcie czynności . . . . . .

   . . . . . .

   . . . . . .

   . . . . . .
8. Wnioski i zalecenia audytowe:. . . . . .

   . . . . . .

   . . . . . .

ADMINISTRATOR DANYCH: INSPEKTOR OCHRONY DANYCH:

…… ……

(data i podpis) (data i podpis)

Przykładowe scenariusze sytuacji podlegających ocenie w ramach procedury naruszeniowej

Scenariusz 1

Przez pomyłkę, podczas aktualizacji listy numerów telefonów do naszych pracowników zmieniliśmy ich kolejność, co odkryto po kilku dniach, gdy przełożony dodzwonił się do innego pracownika niż zamierzono.

Doszło do naruszenia ochrony danych osobowych w postaci naruszenia integralności listy z telefonami pracowników, ale można to w krótkim czasie naprawić, i żaden sposób prawa lub wolności pracowników, których telefony były zawarte na liście nie zostaną naruszone.

Zdarzenie należy odnotować w rejestrze naruszeń, ale nie trzeba zgłaszać go do organu nadzorczego, ani informować pracowników o naruszeniu (brak przewidywanych negatywnych następstw dla osób, których naruszenie dotyczyło).

Scenariusz 2

Wariant a) Zgubiono pendrive z plikiem w formacie Excel, zawierającym listę płac pracowników naszej firmy (z imionami, nazwiskami oraz wskazaniem ile konkretny pracownik zarabia oraz ilością przepracowanych w ostatnim miesiącu godzin). Pendrive nie był zaszyfrowany. Nie wiemy gdzie go zgubiono, nie wiemy kto go znalazł i odczytał. Nie możemy wykluczyć naruszenia poufności. **Zdarzenie należy odnotować w rejestrze naruszeń**, **zgłosić niezwłocznie po potwierdzeniu tego faktu do organu nadzorczego i natychmiastowo poinformować osoby, których wysokość wynagrodzenia znalazła się na utraconym nośniku** o fakcie zagubienia nośnika.

Wariant b) Jeżeli pendrive byłby skutecznie zaszyfrowany (albo plik na nim przechowywany) – **nie trzeba byłoby zgłaszać zdarzenia do organu nadzorczego oraz informować osób, których dane się na nim znajdowały** (pod warunkiem, że na innym urządzeniu lub w innej formie pozostałaby zapisana kopia tej informacji i nie doszłoby do bezpowrotnej utraty dostępności). Zdarzenie powinno być jednak **odnotowane w wewnętrznym rejestrze naruszeń.**

Wariant c) Jeżeli zamiast imion i nazwisk, na dysku przenośnym były zapisane jedynie przypisane pracownikom numery, a klucz umożliwiający przypisanie numeru do pracownika posiadał jedynie dział kadr, nie musielibyśmy zgłaszać naruszenia do organu nadzorczego oraz informować o nim osób, o których informacje się znajdowały na utraconym nośniku (pod warunkiem, że na innym urządzeniu lub w innej formie pozostałaby zapisana kopia tej informacji i nie doszłoby do bezpowrotnej utraty dostępności).Wynika to z faktu, że możliwe byłoby argumentowanie, że osoba, która dysk znajdzie i odczyta, nie będzie miała możliwości przypisania zgromadzonych na nim informacji do konkretnych osób. **Zdarzenie powinno być jednak odnotowane w wewnętrznym rejestrze naruszeń.**

Scenariusz 3

Przed długim weekendem, opuszczając biuro bezpośrednio nad nami, pracownik sąsiedniej firmy zapomniał zakręcić kranu w łazience, w efekcie czego doszło do zalania drewnianej szafy z dokumentami pracowników (umowy, dokumentacja niezbędna dla urzędu skarbowego, ZUSu, do wyliczenia wynagrodzenia, urlopu). W wyniku

zalania, część dokumentów uległa „sklejeniu", co skutkować będzie zniszczeniem części dokumentów podczas ich rozdzielania. **Doszło do naruszenia ochrony danych osobowych w postaci naruszenia dostępnośc**i dokumentacji dotyczącej pracowników, co może być związane z poniesieniem przez nich dodatkowych nakładów w postaci czasu (wizyty w urzędach, odtwarzanie treści części dokumentów, trudności w udokumentowaniu niektórych uprawnień przed organami ubezpieczeniowymi, skarbowymi itd.) **Zdarzenie należy odnotować w rejestrze naruszeń, zgłosić niezwłocznie po potwierdzeniu tego faktu do organu nadzorczego i natychmiastowo poinformować osoby, na temat których dokumenty mogły zostać utracone.**

Scenariusz 4

Przez pomyłkę wysłano zwykłego maila, który miał być skierowany do naszego pracownika – do przypadkowego adresata. W mailu znajdowała się informacja, że w przyszłą środę, o godzinie 10 odbędzie się szkolenie dotyczące zmian w kodeksie pracy. Zdarzenia nie trzeba zgłaszać do organu nadzorczego, nie trzeba też informować osoby, której dane znajdowały się w omyłkowo wysłanym mailu – ponieważ ze skali pomyłki i prozaicznych informacji zawartych w mailu wynika małe prawdopodobieństwo, by przypadkowy odbiorca mógł wykorzystać informacje w nim zawarte do naruszenia jakichkolwiek praw lub wolności prawidłowego adresata. **Zalecane jest odnotowanie zdarzenia w wewnętrznym rejestrze naruszeń.**

Scenariusz 5

Przez pomyłkę wysłaliśmy mail z prywatnymi numerami telefonów naszych pracowników w odpowiedzi na wiadomość, która posiadała w kopii kilkanaście adresów z zewnątrz firmy. W efekcie prywatne numery telefonów pracowników zostały ujawnione osobom nieuprawnionym. Zdarzenie należy **odnotować w rejestrze naruszeń, zgłosić niezwłocznie po potwierdzeniu tego faktu do organu nadzorczego i natychmiastowo poinformować osoby,** których telefony znalazły się w omyłkowo wysłanym mailu.

	POLITYKA OCHRONA DANYCH OSOBOWYCH	Wersja	1.00
		Data opracowania	……...
		Właściciel	……...
SPRAWOZDANIE Z KONTROLI ZGODNOŚCI PRZETWARZANIA DANYCH – WZÓR			Załącznik nr 13

. . . . . .

(miejscowość, data)

Sprawozdanie z kontroli zgodności przetwarzania danych osobowych

1. Oznaczenie Administratora Danych i adres jego siedziby:

   . . . . . .

2. Imię i nazwisko Inspektora Ochrony Danych:

   . . . . . .

3. Wykaz czynności podjętych przez Inspektora Ochrony w toku kontroli oraz imiona, nazwiska i stanowiska osób biorących udział w tych czynnościach:

   . . . . . .

4. Data rozpoczęcia i zakończenia kontroli:

   . . . . . .

5. Określenie przedmiotu i zakresu kontroli:

   . . . . . .

6. Opis stanu faktycznego stwierdzonego w toku kontroli oraz inne informacje mające istotne znaczenie dla oceny zgodności przetwarzania danych z przepisami o ochronie danych:

   . . . . . .

7. Stwierdzone przypadki naruszenia przepisów o ochronie danych osobowych w zakresie objętym kontrolą wraz z planowanymi lub podjętymi działaniami przywracającymi stan zgodny z prawem:

   . . . . . .

8. Wnioski i zalecenia pokontrolne

   . . . . . .

9. Wyszczególnienie załączników stanowiących składową część sprawozdania:

   . . . . . .

ADMINISTRATOR DANYCH: INSPEKTOR OCHRONY DANYCH:

…… ……

(data i podpis) (data i podpis)

	POLITYKA OCHRONA DANYCH OSOBOWYCH	Wersja	1.00
		Data opracowania	……...
		Właściciel	……...
OŚWIADCZENIE O ZOBOWIĄZANIU SIĘ DO PRZESTRZEGANIA ZASAD OCHRONY DANYCH – WZÓR			Załącznik nr 14

. . . . . .

(miejscowość, data)

Oświadczenie o zobowiązaniu się do przestrzegania zasad ochrony danych osobowych

Ja niżej podpisany** . . . . . ,
zam. . . . . ,
Nr Pesel:. . . . . ,
oświadczam, iż w dniu . . . . . zostałam/zostałem* zapoznana/zapoznany* z przepisami dotyczącymi ochrony danych osobowych, oraz wprowadzonymi i wdrożonymi do stosowania przez Administratora Danych dokumentami: Polityka Ochrony Danych Osobowych oraz Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.
Jednocześnie oświadczam, iż jestem upoważniony do przetwarzania danych osobowych zgodnie z Upoważnieniem Administratora Danych.

Zobowiązuję się do:

a) zachowania w tajemnicy danych osobowych przetwarzanych przez Administratora Danych,
b) zachowania w tajemnicy sposobu zabezpieczenia i przetwarzania danych osobowych przetwarzanych u Administratora Danych,
c) nieujawniania danych osobowych podmiotom nieuprawnionym w jakiejkolwiek formie bez zgody Administratora Danych,
d) przestrzegania Polityki Ochrony Danych Osobowych oraz Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych,
e) korzystania z oprogramowania Administratora Danych wyłącznie w związku z wykonywaniem obowiązków pracowniczych,
f) wykorzystywania jedynie legalnego oprogramowania pochodzącego od Administratora Danych,
g) niepodejmowania prób samodzielnego instalowania oprogramowania pochodzącego z innych źródeł,
h) wnoszenia, wynoszenia i użytkowania komputerów przenośnych bądź innych nośników danych wyłącznie za wiedzą i zgodą Administratora Systemu Informatycznego,
i) należytej dbałości o sprzęt i oprogramowanie,
j) należytego zabezpieczania dokumentów papierowych przed nieuprawnionym dostępem, uszkodzeniem lub zniszczeniem,
k) należytego zabezpieczania pomieszczeń, w których przetwarza się dane osobowe.

Naruszenie przez osobę upoważnioną jej podstawowych obowiązków w zakresie wskazanym powyżej, będzie stanowić podstawę do podjęcia przez Administratora Danych przysługujących mu środków prawnych, a w szczególności może stanowić przyczynę uzasadniającą wypowiedzenie przez Administratora Danych umowy lub rozwiązanie tejże umowy bez wypowiedzenia, z winy naruszającego. Naruszenie zasad ochrony danych osobowych może spowodować odpowiedzialność karną, jak również odpowiedzialność odszkodowawczą na zasadach określonych w ustawie o ochronie danych osobowych oraz w przepisach cywilnych.

ADMINISTRATOR DANYCH:	OSOBA SKŁADAJĄCA OŚWIADCZENIE:
.....	.....
(data i podpis)	(data i podpis)

	POLITYKA OCHRONA DANYCH OSOBOWYCH	Wersja	1.00
		Data opracowania	……..
		Właściciel	……..
SPRAWOZDANIE Z KONTROLI ZGODNOŚCI PRZETWARZANIA DANYCH – WZÓR			Załącznik nr 15

Klauzula poufności/ochrony danych osobowych

1. Wykonawca/Zleceniobiorca/Pracownik* zobowiązany jest do zachowania w tajemnicy/poufności warunków niniejszej Umowy oraz wszelkich informacji dotyczących jej wykonywania, jak też wszelkich danych przetwarzanych przez ……, uzyskanych w związku z zawarciem lub wykonywaniem Umowy, które nie zostały podane przez …… do wiadomości publicznej. Nadto, Wykonawca/Zleceniobiorca/Pracownik* zobowiązuje się, w trakcie obowiązywania Umowy, a także po jej wygaśnięciu, wypowiedzeniu, rozwiązaniu bez wypowiedzenia lub odstąpieniu od niej, do zachowania w tajemnicy, nierozpowszechniania, niekopiowania i nieujawniania (nieudostępniania) w jakikolwiek sposób, wszelkich informacji będących danymi osobowymi w rozumieniu relewantnych przepisów, w szczególności 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), (Dz.U.UE.L.2016.119.1), i ustawy o ochronie danych osobowych dotyczących …… oraz podmiotów z nim powiązanych, jak również informacji związanych z jej działalnością oraz podmiotów powiązanych, których niezachowanie w tajemnicy, rozpowszechnianie, kopiowanie lub ujawnienie (udostępnienie) osobie trzeciej mogłoby wyrządzić …… szkodę – bez względu na sposób i formę uzyskania tych informacji (wejścia w ich posiadanie).

2. Ujawnienie informacji niestanowiących danych osobowych podmiotom trzecim wymaga uzyskania pisemnej zgody Administratora Danych ze wskazaniem, komu i jakie informacje zostaną ujawnione. Tajemnicy nie stanowią ogólne informacje, znane oficjalnie, podane do publicznej wiadomości. Nadto tajemnicy nie stanowią informacje, które: (1) zostały prawnie przekazane Wykonawcy/Zleceniobiorcy/Pracownikowi* przez osobę trzecią, bez naruszenia jakichkolwiek zobowiązań o ich nieujawnianiu podjętych w stosunku do ……, (2) zostały ujawnione przez Wykonawcę/Zleceniobiorcę/Pracownika* za uprzednią pisemną zgodą …… (3) zostały przekazane z mocy powszechnie obowiązujących przepisów prawa lub prawomocnego orzeczenia sądowego.

3. Wykonawca/Zleceniobiorca/Pracownik* zobowiązuje się także do zapewnienia zachowania poufności, na zasadach i w zakresie wynikającym z niniejszego paragrafu, przez każdą z osób reprezentujących Wykonawcę/Zleceniobiorcę/Pracownika* i wykonujących w jego imieniu jakiekolwiek czynności wynikającą i związaną z realizacją Umowy. Za naruszenie powyższych postanowień przez osoby, którym informacje zostały przekazane przez Wykonawcę/Zleceniobiorcę/Pracownika* odpowiada on jak za własne naruszenie.

4. W przypadku naruszenia postanowień powyższych w zakresie zachowania poufności, zobowiązuję się zapłacić …… karę umowną w kwocie …… (słownie: ……) zł. za każde naruszenie. Kara ta nie wyklucza możliwości dochodzenia dodatkowego odszkodowania na zasadach ogólnych.

5. Wszelkie stosunki wynikające z niniejszego zobowiązania podlegają prawu polskiemu. Sądem właściwym w sprawach spornych będzie sąd właściwy ze względu na …….

	POLITYKA OCHRONA DANYCH OSOBOWYCH	Wersja	1.00
		Data opracowania	……...
		Właściciel	……...
PROTOKÓŁ USUNIĘCIA DANYCH – WZÓR			Załącznik nr 16

. . . . . .

(miejscowość, data)

Protokół usunięcia danych osobowych

Komisja w składzie:

1. Przewodniczący Komisji: ……

(imię i nazwisko)

2. Członek Komisji ……

(imię i nazwisko)

3. Członek Komisji ……

(imię i nazwisko)

4. Członek Komisji ……

(imię i nazwisko)

dokonała trwałego zniszczenia danych osobowych w ramach procesu danych osobowych o nazwie . . . . . .

. . . . . .

(podmiot danych/nazwa procesu – zbioru danych)

na podstawie . . . . . .

. . . . . .

(podstawa prawna zniszczenia)

Zniszczenie obejmuje:

1. Wersję papierową zbioru. Zniszczenia dokonano poprzez

. . . . . .

(opis sposobu zniszczenia)

2. Bazę danych. Zniszczenia dokonano poprzez

. . . . . .

(opis sposobu zniszczenia)

3. Kopie bezpieczeństwa. Zniszczenia dokonano poprzez

. . . . . .

(opis sposobu zniszczenia)

Dokonanie w/w czynności zostaje potwierdzone własnoręcznymi podpisami komisji:

1. Przewodniczący Komisji: .....
   (imię i nazwisko)
2. Członek Komisji .....
   (imię i nazwisko)
3. Członek Komisji .....
   (imię i nazwisko)
4. Członek Komisji .....
   (imię i nazwisko)

ADMINISTRATOR DANYCH:	INSPEKTOR OCHRONY DANYCH:
.....	.....
(data i podpis)	(data i podpis)

	POLITYKA OCHRONA DANYCH OSOBOWYCH	Wersja	1.00
		Data opracowania	……..
		Właściciel	……..
PROTOKÓŁ PRZEKAZANIA DOKUMENTÓW NA CZAS KONTROLI – WZÓR			Załącznik nr 16

. . . . . .

(miejscowość, data)

Protokół przekazania dokumentów na czas kontroli organu

Wszelkie informacje uzyskane w wyniku: analizy dokumentów, oględzin systemów informatycznych, pomieszczeń, urządzeń, nośników, itp., jak również wszelkie wyjaśnienia przekazane podczas kontroli przeprowadzonej przez uprawnione instytucje, organy, w szczególności osoby je reprezentujące – są poufne i nie mogą być udostępniane inaczej aniżeli na mocy przepisów prawa powszechnie obowiązującego.

Lista przekazanych dokumentów przekazanych na potrzeby kontroli organu*:

1. . . . . .
2. . . . . .
3. . . . . .
4. . . . . .
5. . . . . .
6. . . . . .
7. . . . . .
8. . . . . .
9. . . . . .
10. . . . . .
11. . . . . .

. . . . . .

(data i podpis osoby reprezentującej

Administratora Danych)

Potwierdzam przyjęcie dokumentów

. . . . . .

(data i podpis osoby kontrolującej)

* Listę należy sporządzić w sposób szczegółowy, wyodrębniając każdy przekazany dokument, informacje

	POLITYKA OCHRONA DANYCH OSOBOWYCH	Wersja	1.00
		Data opracowania	……...
		Właściciel	……...
INSTRUKACJA ZARZĄDZANIA KLUCZAMI – WZÓR			Załącznik nr 18

INSTRUKCJA ZARZĄDZANIA KLUCZAMI

Postanowienia ogólne

Instrukcja zarządzania kluczami obejmuje pomieszczenia zlokalizowane . . . . . .
. . . . . .
. . . . . .
. . . . . .

1. Klucze do pomieszczeń pozostają pod osobistym nadzorem osób upoważnionych, które otrzymały klucze za pokwitowaniem.
2. Klucze zapasowe przechowywane są w . . . . . .
   a) Wydawanie kluczy zapasowych upoważnionym pracownikom może odbywać się tylko w uzasadnionych sytuacjach oraz przypadkach awaryjnych za zgodą Administratora Danych;
   b) Klucze zapasowe po ich wykorzystaniu należy niezwłocznie zwrócić do depozytu.
3. Klucze służące do zabezpieczenia biurek i szaf muszą być jednoznacznie opisane.
4. W godzinach pracy klucze pozostają pod nadzorem pracowników, którzy ponoszą pełną odpowiedzialność za ich należyte zabezpieczenie.
5. Zabrania się pozostawiania kluczy w biurkach i szafach.
6. Po zakończeniu pracy, klucze służące do zabezpieczenia biurek i szaf muszą być przechowywane w zabezpieczonym miejscu, lub pod dozorem pracownika.
7. Po zakończeniu pracy, pracownicy są zobowiązani do zabezpieczenia pomieszczeń, a w szczególności wyłączenia i zabezpieczenia urządzeń elektronicznych oraz elektrycznych, wyłączenia oświetlenia, zabezpieczenia i zamknięcia okien i drzwi, ewentualnie aktywacji alarmu.

Postanowienia szczegółowe

W celu zabezpieczenie danych osobowych przed dostępem osób nieuprawnionych Administrator stosuje następującą politykę kluczy:

a) klucze do szuflad i szaf:
   - wszystkie szafy i szuflady, w których przechowywane są nośniki (w szczególności dokumenty) zawierające Dane osobowe zamykane są na klucz;
   - do pobierania kluczy do szuflad i szaf upoważnione są wyłącznie osoby, które zostały upoważnione do przetwarzania Danych osobowych;

- po zakończeniu pracy szafy i szuflady zamykane są na klucz przez ostatnią osobę opuszczającą Dane pomieszczenie lub inną osobę, jeżeli szafa lub szuflada z uzasadnionych względów pozostała otwarta. Przez uzasadnione względy rozumie się w szczególności konieczność dostępu do dokumentów, znajdujących się w danej szafie lub szufladzie;
- klucze do szuflad i szaf przechowywane są w . . . . . ;
- zabrania się wynoszenia kluczy do szuflad i szaf poza . . . . . ;

b) klucze do pomieszczeń i budynku:

- klucze do budynku . . . . . lub do pomieszczeń . . . . . otrzymują wyłącznie osoby upoważnione. Upoważnienie obejmuje również dostęp do budynku i pomieszczeń . . . . . poza godzinami pracy. . . . . (. . . . . .);
- każdy klucz jest imienny i przypisany do konkretnej osoby;
- upoważnienie, o którym mowa w pkt a) powyżej obejmuje umocowanie do korzystania z klucza do pomieszczeń . . . . . .lub budynku bez konieczności jego zdawania;
- Osoba upoważniona ma obowiązek sprawować nadzór na przekazanym kluczem przez cały czas dysponowania nim;
- każde udzielenie lub anulowanie upoważnienia odnotowywane jest w prowadzonej w tym celu ewidencji przekazanych kluczy.

Odpowiedzialność

Naruszenie zasad instrukcji zarządzania kluczami może spowodować odpowiedzialność wynikającą z art. 52 ustawy z 26 czerwca 1974 r. Kodeks Pracy oraz z art. 363 § 1 ustawy z dnia 23 kwietnia 1964 roku Kodeks Cywilny.

. . . . . .

(miejsce, data, podpis osoby reprezentującej Administratora Danych)

Zapoznałem się z treścią Instrukcji zarządzania kluczami i zobowiązuję się do przestrzegania zasad w niej zawartych

. . . . . .

(miejsce, data, podpis pracownika/osoby upoważnionej do posiadania kluczy)

	POLITYKA OCHRONA DANYCH OSOBOWYCH	Wersja	1.00
		Data opracowania	……..
		Właściciel	……..
INSTRUKACJA ZARZĄDZANIA NARUSZENIAMI – WZÓR			Załącznik nr 19

INSTRUKCJA POSTĘPOWANIA W PRZYPADKU NARUSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

Na mocy art. 32 i nast. 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), (Dz.U.UE.L.2016.119.1) wdraża się do stosowania Instrukcję Postępowania w Przypadku Naruszenia Bezpieczeństwa Danych Osobowych.

1. Cel i przedmiot Instrukcji

W związku z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27.04.2016 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 danych) Dz. Urz UE, L 119, str. 1, (dalej „RODO") celem Instrukcji jest określenie sposobu postępowania gdy:

1) Stwierdzono naruszenie danych osobowych lub zabezpieczeń danych osobowych;
2) W przypadku danych przetwarzanych w formie tradycyjnej stan pomieszczeń, szaf, okien, drzwi, dokumentów lub inne zaobserwowane symptomy mogą wskazywać na naruszenie bezpieczeństwa danych osobowych;
3) W przypadku danych przetwarzanych w formie elektronicznej stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu, jakość komunikacji lub inne zaobserwowane symptomy mogą wskazywać na naruszenie bezpieczeństwa danych osobowych.

Instrukcja określa zasady postępowania wszystkich osób zatrudnionych na jakiejkolwiek podstawie przy przetwarzaniu danych osobowych w przypadku naruszenia bezpieczeństwa tych danych, zgodne z „Tabelą form naruszeń bezpieczeństwa danych osobowych", stanowiącą załącznik A do niniejszej Instrukcji.

2. Definicje, symbole, oznaczenia

Administrator – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych

Administrator systemu informatycznego – osoba odpowiedzialna za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemu informatycznego do przetwarzania danych osobowych (może to być administrator sieci lokalnej, systemu operacyjnego, bazy danych itp.).

Dane osobowe – 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.

Inspektor Ochrony Danych (IOD) – osoba, o której mowa w art. 37–39 RODO.

Naruszenie ochrony danych osobowych – 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.

Podmiot przetwarzający – osoba fizyczna lub prawna, organ publiczny, jednostka organizacyjna lub inny podmiot, który przetwarza dane osobowe,– w jego imieniu, w związku z realizacją zobowiązania wykonywanego na rzecz Administratora stosownie do postanowień Umowy powierzenia.

Przetwarzanie – operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taki jak 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.

System informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

3. Definicje incydentu

1) Incydentem w zakresie danych osobowych jest sytuacja powodująca utratę poufności, integralności lub dostępności przetwarzanych danych.
2) Przykładem naruszenia poufności danych osobowych jest nieuprawnione ujawnienie np. wysłanie wiadomości e-mail z załącznikiem zawierającym dane osobowe adresata, który nie powinien jej otrzymać, gdyż był osobą nieuprawnioną do otrzymania przedmiotowej wiadomości.
3) Przykładem naruszenia integralności danych osobowych jest przypadkowe utracenie np. omyłkowe wybranie komendy niszczenia jedynej kopii danych na dysku.
4) Przykładem naruszenia dostępności danych osobowych jest przypadkowe zmodyfikowanie np. omyłkowe wybranie komendy podmieniającej nazwiska osób w jedynej kopii baz danych na jedno i to samo nazwisko „Kowalski" we wszystkich rekordach.
5) Naruszeniem danych osobowych jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia jakiegokolwiek elementu Systemu informatycznego, a w szczególności:
   - nieautoryzowany dostęp do danych,
   - nieautoryzowane modyfikacje lub zniszczenie danych,
   - udostępnienie danych nieautoryzowanym podmiotom,
   - nielegalne ujawnienie danych,
   - pozyskiwanie danych z nielegalnych źródeł.

4. Odpowiedzialność

1) W przypadku stwierdzenia naruszenia danych osobowych lub ich zabezpieczeń albo zaistnienia sytuacji, które mogą wskazywać na naruszenie danych osobowych lub ich zabezpieczeń, każda osoba zatrudniona na jakiejkolwiek podstawie przy przetwarzaniu danych osobowych zobowiązana jest natychmiast
   a) przerwać przetwarzanie danych osobowych,
   b) zabezpieczyć dowody umożliwiające ustalenie przyczyn oraz skutków naruszenia lub zagrożenia,
   c) zgłosić ten fakt bezpośredniemu przełożonemu lub Inspektorowi Ochrony Danych, a następnie postępować stosownie do podjętej przez Inspektora Ochrony Danych decyzji.
2) Przykłady naruszeń oraz szczegółowy tryb postępowań wskazane zostały w „Tabeli form naruszeń bezpieczeństwa danych osobowych", stanowiącej załącznik A do niniejszej Instrukcji.
3) Zgłoszenie, o którym mowa w 5.1 powinno zawierać:
   a) opisanie symptomów naruszenia danych osobowych i ich zabezpieczeń, w tym w miarę możliwości wskazać kategorię i przybliżoną liczbę osób, których dane dotyczą,
   b) określenie sytuacji i czasu w jakim stwierdzono naruszenie lub zagrożenie naruszenia danych osobowych i ich zabezpieczeń,
   c) określenie wszelkich istotnych informacji mogących wskazywać na przyczynę naruszenia,
   d) określenie znanych danej osobie sposobów zabezpieczenia Systemu informatycznego oraz wszelkich kroków podjętych po ujawnieniu zdarzenia.
4) Zgłoszenie powinno być dokonane w formie elektronicznej na adres ……, a jeśli wymaga tego zaistniała sytuacja telefonicznie lub ustnie.
5) Inspektor Ochrony Danych jest odpowiedzialny za analizę incydentów bezpieczeństwa lub zagrożeń ochrony danych osobowych, sporządzenie raportu z incydentu oraz zgłoszenie naruszenia danych osobowych Urzędowi ochrony danych, a także zawiadomienie o naruszeniu osoby, której dane dotyczą – w przypadku ziszczenia się określonych przesłanek.
6) Administrator Systemu Informatycznego jest zobowiązany do informowania Inspektora Ochrony Danych o wszelkich anomaliach w pracy administrowanych przez siebie urządzeń, mogących być przyczyną lub skutkiem incydentu w zakresie danych osobowych.

5. Opis postępowania

1) W przypadku zgłoszenia, o którym mowa w pkt. 5 Instrukcji bezpośrednio przełożony natychmiast:
   a) zapoznaje się z zaistniałą sytuacją oraz podejmuje wszelkie działania mające na celu minimalizację negatywnych skutków zdarzenia, wyjaśnienie okoliczności oraz zabezpieczenie dowodów;
   b) powiadamia Inspektora Ochrony Danych o zgłoszeniu, o którym mowa w pkt 5 oraz przekazuje wszystkie informacje jakie posiada związane ze zdarzeniem.
2) W przypadku zgłoszenia, o którym mowa w pkt 5 Instrukcji oraz uzyskania informacji Inspektor Ochrony Danych lub inna upoważniona przez niego osoba podejmuje wszelkie działania mające na celu:
   a) minimalizację negatywnych skutków zdarzenia,
   b) wyjaśnienie okoliczności zdarzenia,

c) zabezpieczenie dowodów zdarzenia,
d) umożliwienie dalszego bezpiecznego przetwarzania danych,
e) nawiązuje kontakt ze specjalistami zewnętrznymi (jeśli zachodzi taka potrzeba).

3) Inspektor Ochrony Danych lub inna upoważniona przez niego osoba dokumentuje każdy przypadek naruszenia bezpieczeństwa danych sporządzając raport, którego wzór stanowi załącznik B.
4) Inspektor Ochrony Danych lub inna upoważniona przez niego osoba zasięga potrzebnych opinii i proponuje działania naprawcze w każdym przypadku naruszenia bezpieczeństwa danych (w tym także ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych osobowych), wskazując je w rejestrze incydentów i działań korygujących, którego wzór stanowi załącznik C.
5) W przypadku gdy zdarzenie narusza ochronę danych osobowych, Administrator, po konsultacji z Inspektorem Ochrony Danych, bez zbędnej zwłoki w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je Urzędowi ochrony danych, 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. Wzór zgłoszenia stanowi załącznik D do niniejszej Instrukcji.
6) Zgłoszenie, o którym mowa w ust. 4, musi 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.
7) Jeżeli – i w zakresie, w jakim – informacji nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki.
8) 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.
9) Zawiadomienie, o którym mowa w ust. 7, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w ust. 5 lit. b), c) i d). Wzór zawiadomienia stanowi załącznik E.
10) Zawiadomienie, o którym mowa w ust. 7, nie jest wymagane, w następujących przypadkach:
   a) Administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;

b) Administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą;
c) wymagałoby ono niewspółmiernie dużego wysiłku.

11) 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.
12) W celu realizacji zadań wynikających z niniejszej Instrukcji Inspektor Ochrony Danych lub inna upoważniona przez niego osoba ma prawo do podejmowania wszelkich działań dopuszczonych przez prawo, a w szczególności:
a) żądania wyjaśnień od pracowników,
b) korzystania z pomocy konsultantów,
c) nakazania przerwania pracy, zwłaszcza w zakresie przetwarzania danych osobowych.
13) Polecenia Inspektora Ochrony Danych lub innej upoważnionej przez niego osoby wydawane w celu realizacji zadań wynikających z niniejszej Instrukcji są priorytetowe i winny być wykonywane przed innymi poleceniami, zapewniając ochronę danych osobowych.

6. Odpowiedzialność za naruszenia zasad postępowania

1) Niepowiadomienie odpowiedniej osoby, odmowa udzielenia wyjaśnień lub współpracy z Inspektorem Ochrony Danych lub inną upoważnioną przez niego osobą traktowana będzie jako naruszenie obowiązków pracowniczych. Nieprzestrzeganie innych zasad postępowania określonych w niniejszej Instrukcji stanowić może stanowić naruszenie obowiązków pracowniczych i może być przyczyną odpowiedzialności dyscyplinarnej określonej w Kodeksie Pracy.
2) Odpowiedzialność dyscyplinarna z ust. 1 nie wyklucza odpowiedzialności karnej zgodnie z aktualnie obowiązującymi przepisami w tym zakresie.
3) Jeżeli skutkiem działań określonych w ust. 1 jest szkoda, sprawca ponosi odpowiedzialność materialną na warunkach określonych w przepisach Kodeksu Pracy oraz/lub Kodeksu Cywilnego.

7. Postanowienia końcowe

1) Instrukcja jest dokumentem wewnętrznym. Wszyscy upoważnieni do przetwarzania danych osobowych zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w Instrukcji.
2) W sprawach nieuregulowanych w Instrukcji zastosowanie mają przepisy rozporządzenia (RODO), ustawy oraz przepisów wykonawczych do ustawy.

8. Wykaz załączników

A - Tabela form naruszeń bezpieczeństwa danych osobowych
B - Raport z naruszenia ochrony danych
C - Rejestr incydentów i działań korygujących
D - Wzór zgłoszenia naruszenia ochrony danych
E - Wzór zawiadomienia

Tabela form naruszeń bezpieczeństwa danych osobowych

Kod naruszenia	Formy naruszeń	Sposób postępowania
A	**Forma naruszenia ochrony danych osobowych przez pracownika zatrudnionego przy przetwarzaniudanych**	
A.1	**W zakresie wiedzy:**	
A.1.1	Ujawnianie sposobu działania aplikacji i Systemu informatycznego jej zabezpieczeń osobom niepowołanym	Natychmiast przerwać rozmowę lub inną czynność prowadzącą do ujawnienia informacji Powiadomić Inspektora Ochrony Danych Sporządzić raport z opisem, jaka informacja została ujawniona
A.1.2	Ujawnianie informacji o sprzęcie i pozostałej infrastrukturze informatycznej	Natychmiast przerwać rozmowę lub inną czynność prowadzącą do ujawnienia informacji Sporządzić raport z opisem, jaka informacja została ujawniona, powiadomić Inspektora Ochrony Danych
A.1.3	Dopuszczanie i stwarzanie warunków, aby ktokolwiek taką wiedzę mógł pozyskać np. z obserwacji lub dokumentacji	Natychmiast przerwać rozmowę lub inną czynność prowadzącą do ujawnienia informacji. Powiadomić Inspektora Ochrony Danych. Sporządzić raport z opisem, jaka informacja została ujawniona.
A.2	**W zakresie sprzętu i oprogramowania**	
A.2.1	Opuszczenie stanowiska pracy i pozostawienie aktywnej aplikacji umożliwiającej dostęp do danych osobowych	Niezwłocznie zakończyć działanie aplikacji Sporządzić zgłoszenie
A.2.2	Dopuszczenie do korzystania z aplikacji umożliwiającej dostęp do danych osobowych przez jakiekolwiek inne osoby niż osoba, której dostęp został przyznany	Wezwać osobę bezprawnie korzystającą z aplikacji do opuszczenia stanowiska przy komputerze Pouczyć osobę, która dopuściła do takiej sytuacji Sporządzić zgłoszenie
A.2.3	Pozostawienie w niezabezpieczonym, ogólnie dostępnym miejscu hasła dostępu do komputera, Systemów informatycznych przetwarzających dane osobowe lub umożliwiające dostęp do lokalnej sieci komputerowej	Sporządzić raport Niezwłocznie powiadomić Inspektora Ochrony Danych
A.2.4	Dopuszczenie do użytkowania sprzętu komputerowego i oprogramowania umożliwiającego dostęp do danych osobowych przez osoby nie będące uprawnionymi pracownikami	Wezwać osobę nieuprawnioną do opuszczenia stanowiska. Ustalić jakie czynności zostały przez osoby nieuprawnione wykonane Sporządzić raport Niezwłocznie powiadomić Inspektora Ochrony Danych
A.2.5	Samodzielne instalowanie oprogramowania	Pouczyć osobę popełniającą wymienioną czynność, aby jej zaniechała Wezwać personel informatyczny w celu odinstalowania programów Sporządzić zgłoszenie
A.2.6	Modyfikowanie parametrów Systemu informatycznego i aplikacji	Wezwać osobę popełniającą wymienioną czynność, aby jej zaniechała Sporządzić zgłoszenie
A.2.7	Odczytywanie nośników danych przed sprawdzeniem ich programem antywirusowym	Pouczyć osobę popełniającą wymienioną czynność, aby stosowała się do wymogów bezpieczeństwa pracy Wezwać personel informatyczny w celu wykonania skanu antywirusowego. Sporządzić zgłoszenie
A.3	**W zakresie dokumentów zawierających dane osobowe**	
A.3.1	Pozostawienie dokumentów w otwartych pomieszczeniach bez nadzoru	Zabezpieczyć dokumenty Sporządzić zgłoszenie
A.3.2	Przechowywanie dokumentów zabezpieczonych w niedostatecznym stopniu przed dostępem osób niepowołanych	Powiadomić bezpośredniego przełożonego Spowodować poprawienie zabezpieczeń Sporządzić zgłoszenie
A.3.3	Niszczenie dokumentów w stopniu umożliwiającym ich odtworzenie i odczytanie.	Zabezpieczyć niewłaściwie zniszczone dokumenty Powiadomić bezpośredniego przełożonego Sporządzić zgłoszenie
A.3.4	Dopuszczanie do kopiowania dokumentów i utraty kontroli nad kopią	Zaprzestać kopiowania Odzyskać i zabezpieczyć wykonaną kopię Powiadomić bezpośrednio przełożonego Sporządzić zgłoszenie
A.3.5	Umożliwienie odczytu zawartości ekranu monitora, na którym wyświetlane są dane osobowe	Wezwać nieuprawnioną osobę odczytującą dane do zaprzestania czynności Zmienić lokalizację stanowiska pracy, doposażyć stanowisko w filtr prywatyzujący Jeżeli ujawnione zostały dane osobowe sporządzić zgłoszenie
A.3.6	Sporządzanie kopii danych na nośnikach danych w sytuacjach nie przewidzianych procedurą	Spowodować zaprzestanie kopiowania Odzyskać i zabezpieczyć wykonaną kopię Sporządzić raport Powiadomić Inspektora Ochrony Danych

Kod naruszenia	Formy naruszeń	Sposób postępowania
A.3.7	Utrata kontroli nad kopią danych osobowych	Podjąć próbę odzyskania kopii Sporządzić raport Powiadomić Inspektora Ochrony Danych
A.4	**W zakresie pomieszczeń i infrastruktury służących do przetwarzania danych osobowych**	
A.4.1	Opuszczanie i pozostawianie bez dozoru nie zamkniętego pomieszczenia, w którym zlokalizowany jest sprzęt komputerowy używany do przetwarzania danych osobowych (ryzyko dokonania na sprzęcie lub oprogramowaniu modyfikacji zagrażających bezpieczeństwu danych osobowych)	Zabezpieczyć (zamknąć) pomieszczenie Sporządzić zgłoszenie Powiadomić bezpośrednio przełożonego
A.4.2	Wpuszczanie do pomieszczeń osób nieznanych, niepowołanych i dopuszczanie do ich kontaktu ze sprzętem komputerowym	Wezwać osoby bezprawnie przebywające w pomieszczeniach do ich opuszczenia, próbować ustalić ich tożsamość Sporządzić raport Powiadomić bezpośrednio przełożonego oraz Inspektora Ochrony Danych
A.4.3	Dopuszczanie, aby osoby spoza personelu informatycznego podłączały jakikolwiek urządzenia do sieci komputerowej, demontowały elementy obudów gniazd i torów kablowych lub dokonywały jakichkolwiek manipulacji	Wezwać osoby dokonujące zakazanych czynność do ich zaprzestania Postarać się ustalić ich tożsamość Sporządzić raport Powiadomić personel informatyczny oraz Inspektora Ochrony Danych
A.5	**W zakresie pomieszczeń w których znajdują się komputery centralne i urządzenia sieci**	
A.5.1	Dopuszczenie lub ignorowanie faktu, że osoby spoza personelu informatycznego dokonują jakichkolwiek manipulacji przy urządzeniach lub okablowaniu sieci komputerowej w miejscach publicznych (sale konferencyjne, korytarze, open-space itp.)	Wezwać osoby dokonujące zakazanych czynność do ich zaprzestania i ew. opuszczenia pomieszczeń Postarać się ustalić ich tożsamość Sporządzić raport Powiadomić personel informatyczny oraz Inspektora Ochrony Danych
A.5.2	Dopuszczanie do znalezienia się w pomieszczeniach technicznych (serwerownie, cross-roomy) osób spoza personelu informatycznego lub ignorowania takiego faktu	Wezwać osoby dokonujące zakazanych czynność do ich zaprzestania i opuszczenia chronionych pomieszczeń Postarać się ustalić ich tożsamość Sporządzić raport Powiadomić personel informatyczny oraz Inspektora Ochrony Danych
B	**Zjawiska świadczące o możliwości naruszenia ochrony danych osobowych**	
B.1	Ślady ingerencji, manipulacji przy sieci komputerowej lub komputerach	Powiadomić niezwłocznie personel informatyczny oraz Inspektora Ochrony Danych Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji Sporządzić raport
B.2	Obecność instalacji i urządzeń o nieznanym przeznaczeniu i pochodzeniu	Powiadomić niezwłocznie personel informatyczny oraz Inspektora Ochrony Danych Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji Sporządzić raport
B.3	Niezapowiedziane zmiany w wyglądzie lub zachowaniu aplikacji służącej do przetwarzania danych osobowych	Powiadomić niezwłocznie personel informatyczny oraz Inspektora Ochrony Danych Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji Sporządzić raport
B.4	Nieoczekiwane, nie dające się wyjaśnić, zmiany zawartości bazy danych osobowych	Powiadomić niezwłocznie personel informatyczny oraz Inspektora Ochrony Danych Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji Sporządzić raport
B.5	Niesygnalizowana obecność nowych aplikacji i programów w komputerze lub inne zmiany w konfiguracji oprogramowania	Powiadomić niezwłocznie personel informatyczny oraz Inspektora Ochrony Danych Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji Sporządzić raport
B.6	Ślady włamania do pomieszczeń, w których przetwarzane są dane osobowe	Powiadomić niezwłocznie Inspektora Ochrony Danych oraz bezpośredniego przełożonego Sporządzić raport
C	**Formy naruszenia ochrony danych osobowych przez personel informatyczny w kontaktach z użytkownikiem**	
C.1	Próba uzyskania hasła uprawniającego do dostępu do danych osobowych w ramach pomocy technicznej	Powiadomić Inspektora Ochrony Danych Sporządzić raport
C.2	Próba nieuzasadnionego dostępu (przeglądania, modyfikowania) w ramach pomocy technicznej danych osobowych za pomocą aplikacji w bazie danych identyfikatorem i hasłem użytkownika	Powiadomić Inspektora Ochrony Danych Sporządzić raport
D.	Inne formy naruszenia ochrony danych osobowych	Powiadomić Inspektora Ochrony Danych Sporządzić raport

Raport o sytuacji naruszenia bezpieczeństwa danych osobowych – wzór

Sporządzający raport:

Imię i nazwisko: ....
stanowisko (funkcja) ....
Dział, pokój, nr telefonu ....
Kod formy naruszenia ochrony danych ....(wg tabeli)

1. Miejsce, dokładny czas i data naruszenia ochrony danych (piętro, nr pokoju, godzina, nazwa programu, aplikacji itp.): ....
2. Osoba powiadamiająca o naruszeniu (imię, nazwisko, stanowisko służbowe): ....
   ....
3. Osoby odpowiedzialne za naruszenie (które swoim działaniem lub zaniechaniem przyczyniły się do naruszenia): ....
   ....
4. Osoby, które uczestniczyły w zdarzeniu związanym z naruszeniem ochrony danych osobowych: ....
   ....
5. Informacje o danych, które zostały lub mogły zostać ujawnione: ....
   ....
6. Zabezpieczone materiały lub inne dowody związane z wydarzeniem:. ....
   ....
7. Krótki opis wydarzenia związanego z naruszeniem ochrony danych osobowych (przebieg zdarzenia, opis zachowania uczestników, podjęte działania): ....
   ....
8. Wnioski: ....
   ....

....

(miejsce, data i godzina sporządzenia raportu) (data i podpis Inspektora Ochrony Danych)

....

(data i podpis zawiadamiającego)

Rejestr incydentów i działań korygujących

Lp.	Data ujawnienia incydentu	Data incydentu	Opis incydentu	Konsekwencje	Podjęte działania naprawcze	Data podjętych działań	Data wdrożenia działań	Osoba odpowiedzialna za wdrożenie działań
1.								
2.								
3.								
4.								
5.								
6.								
7.								

Zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu – wzór

1. Data …… Godzina …… (naruszenia)
2. Osoba powiadamiająca o naruszeniu oraz inne osoby zaangażowane lub odpytane w związku z naruszeniem (imię, nazwisko, stanowisko służbowe,):

   . . . . . .
3. Lokalizacja zdarzenia (nr. pokoju, nazwa pomieszczenia, określenie komputerowego stanowiska roboczego, nazwa programu lub aplikacji itp.):. . . . . .

   . . . . . .
4. Rodzaj naruszenia i określenie okoliczności towarzyszących naruszeniu: . . . . . .

   . . . . . .
5. Podjęte działania:. . . . . .

   . . . . . .
6. Wstępna ocena przyczyn wystąpienia naruszenia (*opisywać możliwe konsekwencje naruszenia ochrony danych osobowych);*

   . . . . . .
7. Postępowanie wyjaśniające i naprawcze (*opisywać środki zastosowane lub proponowane w celu zminimalizowania jego ewentualnych negatywnych skutków);*

   . . . . . .
8. Imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji:

   . . . . . .

. . . . . .

(data i podpis Administratora Danych)

Zawiadomienie osoby fizycznej której dane zostały naruszone o naruszeniu ochrony danych – wzór

. . . . . .

(imię i nazwisko osoby fizycznej której dane zostały naruszone oraz dane kontaktowe tej osoby)

1. Data …… Godzina …… (naruszenia)
2. Osoba powiadamiająca o naruszeniu oraz inne osoby zaangażowane lub odpytane w związku z naruszeniem (imię, nazwisko, stanowisko służbowe,):

   . . . . . .
3. Lokalizacja zdarzenia (nr. pokoju, nazwa pomieszczenia, określenie komputerowego stanowiska roboczego, nazwa programu lub aplikacji itp.):

   . . . . . .
4. Rodzaj naruszenia i określenie okoliczności towarzyszących naruszeniu (*opisać 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);*

   . . . . . .
5. Podjęte działania:

   . . . . . .
6. Wstępna ocena przyczyn wystąpienia naruszenia (*opisywać możliwe konsekwencje naruszenia ochrony danych osobowych);*

   . . . . . .
7. Postępowanie wyjaśniające i naprawcze (*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);*

   . . . . . .
8. Imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji:

   . . . . . .

. . . . . .

(data i podpis Administratora Danych)

	POLITYKA OCHRONA DANYCH OSOBOWYCH	Wersja	1.00
		Data opracowania	……...
		Właściciel	……...
ANALIZA RYZYKA – WZÓR			Załącznik nr 20

. . . . . .

(miejscowość, data)

Analiza ryzyka – metodologia

DEFINICJE

1. **Aktywa** – jest to wszystko, co ma wartość dla organizacji (administratora danych lub podmiotu przetwarzającego), np. dane osobowe.
2. **Aktywa podstawowe** – są to procesy, działania biznesowe oraz informacje związane z funkcjonowaniem organizacji (w tym dane osobowe).
3. **Aktywa wspierające –** są to środki umożliwiające korzystanie z aktywów podstawowych. Przykładem aktywów wspierających jest sprzęt, oprogramowanie, sieć, pracownicy.
4. **Anonimizacja –** oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było przypisać konkretnej osobie, której dane dotyczą, za pomocą dodatkowych informacji lub wszelkich innych środków, jakimi dysponuje administrator lub podmiot przetwarzający. Zabieg ten ma charakter trwały i nieodwracalny, powodujący, że po jego przeprowadzeniu nie mamy do czynienia z danymi osobowymi.
5. **Identyfikowanie ryzyka** – jest to czynność polegająca na określeniu, co może się zdarzyć (kiedy, gdzie, jak i dlaczego) i spowodować stratę.
6. **Kontekst** – są to wszystkie informacje wiążące się z działaniem organizacji, m.in. informacje dotyczące środowiska prawnego, społecznego, politycznego, finansowego czy też technologicznego, np. przepisy dotyczące ochrony danych osobowych.
7. **Kryteria akceptacji ryzyka** – są to kryteria, które określają dopuszczalność danego ryzyka. Zwykle definiuje się je poprzez wartość progową.
8. **Kryteria oceny ryzyka** – są to kryteria, które określają poziomy odniesienia, względem których określa się ważność ryzyka.
9. **Naruszenie ochrony danych osobowych –** oznacza 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.
10. **Ocena ryzyka** – jest to czynność polegająca na porównaniu wyników uzyskanych podczas analizy ryzyka z kryteriami oceny ryzyka określonymi na etapie ustanawiania kontekstu działania organizacji.
11. **Operacja przetwarzania danych osobowych** – każda czynność wykonywana na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taka jak 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.

12. **Podatność** – jest to słabość, która może być wykorzystana przez zagrożenie, powodując niekorzystne skutki, np. luka w systemie informatycznym.
13. **Proces przetwarzania danych osobowych** – zespół operacji (czynności) wykonywanych na danych osobowych lub zestawach danych osobowych w celu osiągnięcia określonego celu przetwarzania.
14. **Pseudonimizacja** – oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji. Te dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. W przeciwieństwie do anonimizacji, której skutkiem jest nieodwracalne uniemożliwienie identyfikacji osoby, pseudonimizacja jest procesem odwracalnym.
15. **Ryzyko** – wpływ niepewności na cele. W przypadku ryzyka naruszenia praw i wolności osób, których dane dotyczą, celem będzie ochrona tych praw i wolności.
16. **Szacowanie ryzyka** – całościowy proces identyfikacji ryzyka, analizy ryzyka oraz oceny ryzyka.
17. **Właściciel aktywów –** jest to osoba odpowiedzialna w danym podmiocie za konkretny proces przetwarzania danych i mająca prawo do podejmowania w tym zakresie decyzji, np. dyrektor departamentu, kierownik określonej komórki w organizacji.
18. **Zabezpieczenie** – jest to środek, którego celem jest zmniejszenie ryzyka poprzez obniżenie prawdopodobieństwa zrealizowania zagrożenia (czyli wykorzystania istniejącej podatności) lub też minimalizację potencjalnych strat związanych ze zrealizowanym zagrożeniem, np. program antywirusowy, drzwi antywłamaniowe, stosowanie procedury bezpieczeństwa.
19. **Zagrożenie** – jest to źródło potencjalnej szkody, np. zagrożenie naruszenia integralności danych.

ORGANIZACJA ZARZĄDZANIA RYZYKIEM

1. Nadzór nad procesem zarządzania ryzykiem sprawuje Administrator Danych.
2. Zespół ds. analizy ryzyka Administratora podejmuje decyzje dotyczące:
   1) kryteriów szacowania skutków, oceny ryzyka oraz akceptowania ryzyka,
   2) akceptowania planu postępowania z ryzykiem,
   3) programu systematycznego przeglądu ryzyka w stałym cyklu przeglądowym.
3. Do szczegółowych zadań Zespołu ds. analizy ryzyka u Administratora w zakresie metodyki szacowania ryzyka należy:
   1) inicjowanie zmian w metodyce,
   2) analizowanie znaczących zmian w obszarze ryzyka związanego z bezpieczeństwem informacji,
   3) zatwierdzanie zmian w systemie zarządzania bezpieczeństwem informacji doskonalących proces zarządzania ryzykiem.
4. Kierownik komórki właściwej ds. bezpieczeństwa informacji realizuje i koordynuje działania w procesie zarządzania ryzykiem.

5. Do szczegółowych zadań kierownika komórki właściwej ds. bezpieczeństwa informacji w obszarze systemu zarządzania bezpieczeństwem informacji należy:
   1) doskonalenie metodyki szacowania ryzyka oraz rekomendacji przedstawianych Zespołowi dotyczących zmian w metodyce,
   2) doskonalenie kryteriów szacowania następstw, oceny ryzyka i akceptowania ryzyka oraz rekomendacji przedstawianych Zespołowi dotyczących zmian kryteriów,
   3) rozwój narzędzi wspierających szacowanie ryzyk,
   4) opracowywanie programów przeglądu ryzyka,
   5) koordynowanie działań związanych z zarządzaniem ryzyka, wymagających uczestnictwa komórek organizacyjnych Administratora lub podmiotów zewnętrznych,
   6) wraz z Właścicielami Procesów / Właścicielami Zasobów przygotowanie, uzgadnianie i uaktualnienie planów postępowania z ryzykiem,
   7) przygotowywanie raportów dotyczących ryzyka i planu postępowania z ryzykiem,
   8) szkolenie Właścicieli Procesów / Właścicieli Zasobów oraz innych kierowników komórek organizacyjnych u Administratora w zakresie metodyki szacowania ryzyka,
   9) monitorowanie zmian elementów ryzyka, w szczególności zagrożeń podatności, warunków (wewnętrznych i zewnętrznych) funkcjonowania systemów informacyjnych Administratora mających wpływ na proces zarządzania ryzykiem,
   10) formułowanie rekomendacji dotyczących doskonalenia procesu zarządzania ryzykiem,
   11) realizowanie działań z zakresu informacji zarządzania ryzykiem przypisanych kierownikowi komórki właściwej ds. bezpieczeństwa informacji w dokumentach niższego poziomu.
6. Właściciele Procesów / Właściciele Zasobów oraz, w razie potrzeby, inni kierownicy komórek organizacyjnych realizują programy przeglądów ryzyka w zakresie:
   1) identyfikacji i klasyfikacji zasobów na potrzeby szacowania ryzyka,
   2) identyfikacji scenariuszy incydentów,
   3) szacowania następstw dla zasobów użytych w realizacji procesów objętych przeglądem ryzyka.
7. Właściciele Procesów / Właściciele Zasobów oraz, w razie potrzeb, inni kierownicy komórek organizacyjnych udzielają niezbędnych informacji kierownikowi komórki właściwej ds. bezpieczeństwa informacji w zakresie identyfikowania podatności, zagrożeń oraz zmian warunków funkcjonowania zasobów mających wpływ na szacowanie ryzyka. W tym celu spośród podległych sobie pracowników wyznaczają osoby do roboczych kontaktów z komórką podległą kierownikowi komórki właściwej ds. bezpieczeństwa informacji.

PLAN POSTĘPOWANIA Z RYZYKIEM

1. Kierownik komórki właściwej ds. bezpieczeństwa informacji opracowuje wg propozycji Właścicieli Zasobów plan postępowania z ryzykiem na podstawie wyników szacowania ryzyka oraz zatwierdzonych kryteriów oceny ryzyka.
2. Plan postępowania z ryzykiem podlega akceptacji przez Administratora.

3. Przed przedłożeniem do Zespołu planu postępowania z ryzykiem kierownik komórki właściwej ds. bezpieczeństwa informacji ma obowiązek skonsultowania proponowanych wariantów z Właścicielami Procesów / Właścicielami Zasobów lub, w razie potrzeb, z innymi kierownikami komórek organizacyjnych i uzyskania oceny wykonalności.
4. W przypadku negatywnej oceny wykonalności proponowanego wariantu postępowania z ryzykiem Właściciel Procesu / Właściciel Zasobu lub, w razie potrzeb, inny kierownik komórki organizacyjnej przedstawia pisemne uzasadnienie.

AKCEPTOWALNE RYZYKA

1. Określone ryzyka szczątkowe zawarte w planie postępowania z ryzykiem akceptują Właściciele Zasobów lub, w razie potrzeb, inni kierownicy komórek organizacyjnych pod warunkiem, że Zespół zawarł takie uprawnienie podczas zatwierdzenia konkretnego programu szacowania ryzyka, a wartość oszacowanego ryzyka szczątkowego nie przekracza wartości progowej kryterium akceptowania ryzyka dla Zespołu.
2. W przypadku, gdy wartości ryzyk szczątkowych przekraczają kryterium akceptowania ryzyka dla Zespołu analizy ryzyka przedkłada tę część planu postępowania z ryzykiem Administratora z rekomendacją dalszego postępowania.

INFORMOWANIE O RYZYKU

1. Zagadnienia dotyczące natury i specyfiki ryzyka, charakterystycznych dla działań związanych z realizacją zadań ustawowych bądź statutowych Administratora, są obowiązkowym elementem szkoleń pracowników z zakresu bezpieczeństwa informacji.
2. Kierownik komórki właściwej ds. bezpieczeństwa informacji oraz Właściciele Zasobów i, w razie potrzeb, inni kierownicy komórek organizacyjnych mają obowiązek niezwłocznego informowania, z zachowaniem drogi służbowej obowiązującej, o pojawiających się nowych zagrożeniach, podatnościach systemów informacyjnych Administratora lub zmieniających się uwarunkowaniach funkcjonowania tych systemów, które mogą mieć wpływ na poziom szacowanego ryzyka lub plan postępowania z ryzykiem.
3. Kierownik komórki właściwej ds. bezpieczeństwa informacji przedstawia informację o aktualnym stanie realizacji zatwierdzonych programów szacowania ryzyka na każdym posiedzeniu Zespołu.
4. Identyfikowanie i szacowanie ryzyk związanych z bezpieczeństwem informacji jest obowiązkowym elementem opinii kierownika komórki właściwej ds. bezpieczeństwa informacji załączanej do projektów umów zawieranych przez Administratora oraz wewnętrznych aktów normatywnych.
5. Administrator otrzymuje od Zespołu okresowy raport dotyczący ryzyka związanego z bezpieczeństwem informacji.

KLASYFIKACJA PROCESÓW I ZASOBÓW DLA POTRZEB ZARZĄDZANIA RYZYKIEM

1. Zasoby są niezbędne do realizacji procesów Administratora.
2. Do zasobów Administratora zalicza się:
   1) zasoby informacyjne w formie dokumentacji, baz danych, zbiorów danych osobowych, zbiorów dokumentów źródłowych, itp.:

a) informacje o charakterze strategicznym z punktu widzenia realizacji celów ustawowych bądź statutowych,
b) dane osobowe i inne informacje prawnie chronione,
c) informacje – tajemnice przedsiębiorstwa,
d) informacje o dużym koszcie pozyskania, wymagające długotrwałego przechowywania.

2) infrastrukturę, tzn. zasoby o charakterze technicznym, obejmujące:
a) sprzęt – urządzenia służące do przetwarzania danych:
- serwery, stacje robocze, laptopy,
- urządzenia peryferyjne (np. drukarki, faksy),
- stacjonarne urządzenia do przechowywania danych (np. biblioteki taśmowe),
- wymienne nośniki komputerowe,
- inne nośniki informacji (w tym wydruki papierowe),

b) sieć składającą się z:
- urządzeń telekomunikacyjnych używanych do połączenia odległych elementów systemu teleinformatycznego (pasywnych lub aktywnych – np.: routery, przełączniki, koncentratory, firewalle sprzętowe i aplikacyjne, load balancery itp.),
- mediów transmisyjnych, protokołów i urządzeń teletransmisyjnych (np. publiczna sieć komutowana, Giga Ethernet, ADSL),
- interfejsów telekomunikacyjnych i adapterów (np. GPRS, Ethernet),

3) siedzibę składającą się ze wszystkich fizycznych konstrukcji, instalacji oraz systemów wspomagających, umożliwiających działanie systemów informatycznych, w tym:
a) infrastruktura biurowa,
b) systemy wspomagające (łącza telekomunikacyjne, zasilanie, systemy wentylacyjno-klimatyzacyjne, wodno-kanalizacyjne, ogrzewanie, itp.).

4) zasoby niematerialne, intelektualne i prawne, do których zalicza się:
c) systemy operacyjne,
d) oprogramowanie serwisowe, narzędziowe lub administracyjne,
e) oprogramowanie standardowe (tzw. ofoliowane),
f) aplikacje biznesowe (standardowe lub dedykowane),
g) struktura organizacyjna,
h) instrukcje, procedury, regulaminy, itp.

5) zasoby ludzkie, czyli personel składający się ze wszystkich grup osób zaangażowanych w realizowany proces lub działalność, w tym:
i) osoby decyzyjne, kierownictwo (np.: Właściciele Zasobów / Właściciele Procesów),
j) użytkownicy,
k) operatorzy i administratorzy,
l) projektanci systemów, itp.

3. Klasyfikacja procesów przedstawia się następująco:

1) procesy główne, w których realizowane są zadania statutowe, zwane są one także procesami statutowymi;
2) procesy pomocnicze, które tworzą środowisko niezbędne do realizacji procesów głównych (systemy informatyczne, administracyjne, organizacyjne, itp.).

KRYTERIA SZACOWANIA RYZYKA

1. Prawdopodobieństwo zrealizowania się scenariusza incydentu obejmuje szacowanie dwóch składników: prawdopodobieństwa występowania zagrożenia oraz charakterystyki podatności zasobów informacyjnych.
2. Prawdopodobieństwo wystąpienia zagrożenia jest szacowane w oparciu o charakterystykę zagrożeń specyficzną dla danego systemu zarządzania bezpieczeństwem informacji.
3. Przykładowy wykaz zagrożeń przedstawiono w załączniku.
4. Przy szacowaniu prawdopodobieństwa wystąpienia zagrożenia należy uwzględnić:
   1) charakterystykę zagrożeń (jak często występują, zgodnie z doświadczeniem, dającymi się do zastosowania statystykami itp.),
   2) motywację, czyli zmienne w czasie możliwości (przewidywane i potrzebne), postrzeganie atrakcyjności oraz podatności zasobów dla potencjalnego atakującego – dla źródeł zagrożeń rozmyślnych,
   3) czynniki geograficzne jak bliskość źródeł zagrożeń środowiskowych, możliwość wystąpienia ekstremalnych warunków pogodowych oraz czynniki wpływające na błędy ludzkie i awarie urządzeń – dla źródeł zagrożeń przypadkowych.
5. Dla celów szacowania ryzyka przyjmuje się następujące wielkości prawdopodobieństwa zagrożeń: **1 – zagrożenie niskie**, **2 – zagrożenie średnie**, **4 – zagrożenie wysokie**.

SKALA WARTOŚCI ZAGROŻENIA		
Punktowa	**Opisowa**	**Opis**
1	**NISKIE**	Zagrożenia jest minimalne lub wręcz niezauważalne.
2	**ŚREDNIE**	Wystąpienie zagrożenia może spowodować np. pozew cywilny osoby, której dane dotyczą lub skargę do organu nadzorczego.
4	**WYSOKIE**	Wystąpienie zagrożenia spowoduje kontrolę organu nadzorczego, stratę finansową, utratę wizerunku.

SZACOWANIE PODATNOŚCI

1. Podatności zasobów informacyjnych są analizowane w kontekście istniejących zabezpieczeń i odzwierciedlają łatwość ich wykorzystania przez zagrożenie.
2. Przykładowy wykaz podatności przedstawiono w załączniku.
3. Przyjmuje się następujące parametry analizowanych zabezpieczeń:
   1) zabezpieczenie zostało wdrożone i funkcjonuje, a jego skuteczność została potwierdzona – podatność w danym punkcie należy określić jako „***niską***”,
   2) zostały zidentyfikowane słabości zabezpieczenia, zabezpieczenie zostało uznane za częściowo wdrożone lub nieskuteczne – dla tego zabezpieczenia podatność uznaje się za „***średnią***”,
   3) nie ma zabezpieczenia lub istniejące jest nieskuteczne lub nie funkcjonuje należycie – dla tego zabezpieczenia podatność uznaje się za „***dużą***”.

4. Dla celów szacowania ryzyka przyjmuje się następujące wielkości podatności zasobów informacyjnych: **1 – podatność niska**, **2 – podatność średnia**, **4 – podatność wysoka**.

SKALA WARTOŚCI PODATNOŚCI		
Punktowa	**Opisowa**	**Opis**
1	**NISKIA**	Zabezpieczenie zostało wdrożone i funkcjonuje, a jego skuteczność została potwierdzona
2	**ŚREDNIA**	Zostały zidentyfikowane słabości zabezpieczenia, zabezpieczenie zostało uznane za częściowo wdrożone lub nieskuteczne
4	**WYSOKA**	Nie ma zabezpieczenia lub istniejące jest nieskuteczne lub nie funkcjonuje należycie

ANALIZA RYZYKA

1. Ryzyka przybierają wartości z następujących przedziałów liczb naturalnych:
   1) następstwa dla zasobów informacyjnych {1,...,6},
   2) charakterystyka zagrożenia {1, 2, 4},
   3) charakterystyka podatności (z uwzględnieniem istniejących zabezpieczeń) – {1, 2, 4}.

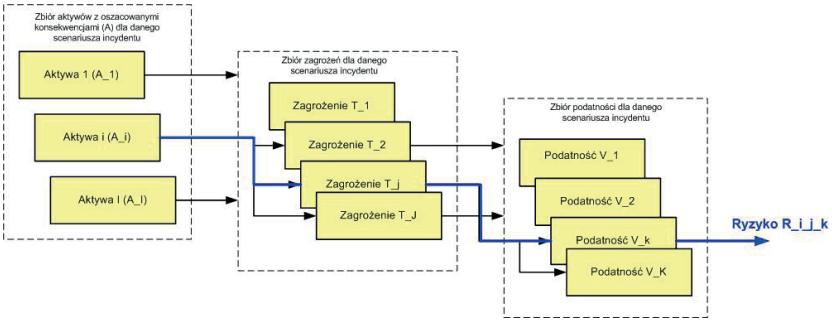
2. Dla każdego scenariusza incydentu (kategorii ryzyka) ryzyko jest kalkulowane dla każdego składnika zbioru zasobów w następujący sposób:

$$A_i \times pr\,(T_j \times V_k) = R_{ijk}$$

gdzie:

A_i – jest wielkością następstw konsekwencji szacowanych dla danego składnika (a_i) zbioru zasobów, $pr\,(T_j \times V_k)$ – prawdopodobieństwo, że dane zagrożenie T_j wykorzysta podatność V_k składnika a_i zbioru zasobów i w efekcie zmaterializuje się scenariusz.

Należy szczególnie podkreślić, że ryzyko dla scenariusza incydentu stanowi zbiór ryzyk, z których każde realizuje ten scenariusz. Miarą tego ryzyka jest kombinacja prawdopodobieństwa wystąpienia scenariusza oraz jego konsekwencji w odniesieniu do konkretnego składnika ze zbioru zasobów. Na Rysunku przedstawiono przykład szacowania ryzyka dla jednego ryzyka ze zbioru, jakie powstają dla każdego scenariusza incydentu. Dla danego zasobu (a_i) są szacowane konsekwencje (A_i) zmaterializowania się – z określonym prawdopodobieństwem – scenariusza, w którym zagrożenie T_j wykorzysta podatność V_k, powodując wynikowe ryzyko R_{ijk}.



Rysunek: Przykład powstania ryzyka dla danego scenariusza incydentu

OCENA RYZYKA

1. Maksymalny poziom ryzyka dla wynosi **96**. Z charakterystyki funkcji ryzyka wynika, że w przypadku Administratora należy podjąć działania w ramach postępowania z ryzykiem, jeśli wartość ryzyka przekroczy **25%** poziomu maksymalnego, czyli **24**.
2. Podane w ust. 1 wartości progowe podlegają weryfikacji w ramach procesu zarządzania bezpieczeństwem informacji oraz samego procesu zarządzania ryzykiem. Wartości progowe mogą być modyfikowane w miarę zidentyfikowanych potrzeb Administratora.

WARTOŚĆ	POZIOM RYZYKA
< 1 – 24 >	NISKI poziom ryzyka utraty bezpieczeństwa danych. Niskie szkody w przypadku realizacji zagrożenia i niska możliwość jego wystąpienia.
< 25 – 48 >	ŚREDNI poziom ryzyka utraty bezpieczeństwa danych. Wysokie szkody w przypadku realizacji zagrożenia i niska możliwość jego realizacji bądź niskie szkody w przypadku realizacji zagrożenia i wysoka możliwość jego realizacji.
< 49 – 72 >	WYSOKI poziom ryzyka utraty bezpieczeństwa danych. Wysokie szkody w przypadku realizacji zagrożenia i wysoka możliwość jego wystąpienia.
< 73 – 96 >	MAKSYMALNY poziom ryzyka utraty danych bezpieczeństwa. Wysokie szkody w przypadku realizacji zagrożenia oraz wysoka możliwość jego wystąpienia, skutkująca nie tylko na organizację, ale na podmioty trzecie.

POSTĘPOWANIE Z RYZYKIEM

Po oszacowaniu ryzyka dla poszczególnych operacji przetwarzania należy podjąć decyzję dotyczącą poszczególnych ryzyk. W normie ISO/IEC 27005 wyróżnia się 4 możliwe rodzaje postępowań. Są to:

1. **modyfikowanie (redukcja) ryzyka** – polega na obniżeniu poziomu ryzyka (np. poprzez zmianę prawdopodobieństwa wystąpienia określonego zdarzenia lub zmniejszenie skutków jego wystąpienia). Na przykład zmniejszenie prawdopodobieństwa wystąpienia zdarzenia spowodowanego przerwą w dostawie energii można osiągnąć, włączając w układ zasilania odpowiednią automatykę i niezależne źródła energii (UPS-y, generatory). Zaś zmniejszenie związanych z tym zdarzeniem skutków utraty danych można osiągnąć, modyfikując system wykonywania kopii z wersji, w której kopia wykonywana jest jeden raz na dobę, do postaci, w której kopia jest wykonywana co 15 minut lub w sposób ciągły (na bieżąco) poprzez zastosowanie dodatkowych zabezpieczeń lub modyfikację procedur w sposób pozwalający na zaakceptowanie ryzyka szczątkowego;
2. **zachowanie (akceptacja) ryzyka** – to świadoma i obiektywna decyzja o niewprowadzaniu żadnych zmian w działaniu organizacji (zabezpieczeń), jeżeli poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka;
3. **unikanie ryzyka** – polega na unikaniu przez organizację działań, które powodują powstanie określonych typów ryzyka, np. w przypadku, gdy zidentyfikowane ryzyka są zbyt wysokie lub koszt wdrożenia zabezpieczeń nie jest adekwatny do zysków;
4. **dzielenie (przeniesienie) ryzyka** – polega na wykupieniu ubezpieczenia od jakiegoś zdarzenia lub scedowaniu skutków ryzyka na kontrahenta (np. podwykonawcę); należy pamiętać, że przeniesienie ryzyka nie eliminuje go. Trzeba zaznaczyć, że zgodnie z przepisami ogólnego rozporządzenia o ochronie danych wykupienie ubezpieczenia nie wyeliminuje ryzyka niezastosowania się przez dany podmiot do przepisów RODO. Ponadto administrator w sytuacji, kiedy zleca innym podmiotom przetwarzanie

danych, to jako podmiot decydujący o zakresie i celach tego przetwarzania, ponosi pełną odpowiedzialność za zgodne z prawem przetwarzanie wskazanych danych.

Akceptowanie ryzyka przez Zespół następuje w przypadku, gdy w planie postępowania z ryzykiem wartości szacowane dla ryzyka szczątkowego będą mniejsze lub równe **25%** poziomu maksymalnego, czyli **24.**

W przypadku, gdy oszacowane ryzyko szczątkowe będzie miało wartość wyższą niż wartość progową, decyzję w sprawie zaakceptowania ryzyka jest przekazywana przez Zespół do Administratora wraz z rekomendacjami.

Rekomendacje zawierają dodatkową charakterystykę ryzyka:

1. rodzaj ryzyka (poziom ryzyka jest akceptowany, jeśli jest to ryzyko materialne, nie może być akceptowane, jeśli dotyczy następstw prawnych lub utraty wizerunku),
2. długość okresu, w którym ryzyko będzie utrzymywać się na wskazanym poziomie (czas, po którym realizacja wariantu postępowania z ryzykiem, będzie możliwa),
3. zasoby i nakłady, jakie trzeba przewidzieć w budżecie i strukturze organizacyjnej, aby wariant postępowania z ryzykiem stał się realizowalny.

* * * *

	INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH	Wersja	1.00
		Data opracowania	……..
		Właściciel	……..
NADANIE UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM – WZÓR			Załącznik nr 1

. . . . . .

(miejscowość, data)

Nadanie uprawnień w systemie informatycznym

Wniosek

Wnoszę o nadanie uprawnień dostępu do systemu informatycznego członkowi personelu/pracownikowi:

. . . . . .

(*Nowy użytkownik / Modyfikacja uprawnień / Odebranie uprawnień w systemie informatycznym**)

Proszę a nadanie następujących uprawnień użytkownika w systemie informatycznym:

. . . . . .

(Opis zakresu uprawnień użytkownika w systemie informatycznym)

1. . . . . ,
2. . . . . ,
3. . . . . ,

Uzasadnienie:

. . . . . .
. . . . . .
. . . . . .
. . . . . .

. . . . . .

(Data i podpis Inspektora Ochrony Danych)

Nadanie uprawnień

Nadaję uprawnienia jak w powyżej opisanym wniosku

. . . . . .

(Data i podpis Administratora Systemu Informatycznego)

*niepotrzebne skreślić

	INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH	Wersja	1.00
		Data opracowania	……..
		Właściciel	……..
PRZEKAZANIE PARAMETRÓW UWIERZYTELNIANIA W SYSTEMIE INFORMATYCZNYM – WZÓR			Załącznik nr 2

. . . . . .

(miejscowość, data)

Przekazanie parametrów uwierzytelniania w systemie informatycznym

Nadaję parametry uwierzytelniania w Systemie Informatycznym

. . . . . .

użytkownikowi:

. . . . . .

(*Nowy użytkownik / Modyfikacja uprawnień / Odebranie uprawnień w systemie informatycznym**)

jak następuje:

Identyfikator (login):

. . . . . .

Hasło jednorazowe:

. . . . . .

. . . . . .

(data i podpis Administratora Systemu Informatycznego)

Potwierdzam

. . . . . .

(Data i podpis Administratora Systemu Informatycznego)

*niepotrzebne skreślić

	INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH	Wersja	1.00
		Data opracowania	……..
		Właściciel	……..
REJESTR UŻYTKOWNIKÓW I UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM – WZÓR			Załącznik nr 3

. . . . . .

(miejscowość, data)

Rejestr użytkowników i uprawnień w systemie informatycznym

L.p.	Imię i nazwisko	Identyfikator użytkownika	Zakres upoważnienia	Data nadania uprawnień	Data i przyczyna odebrania uprawnień
1.					
2.					
3.					
4.					
5.					
6.					
7.					

. . . . . .

(data i podpis Administratora Systemu Informatycznego)

*niepotrzebne skreślić

	INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH	Wersja	1.00
		Data opracowania	……..
		Właściciel	……..
POWOŁANIE ADMINISTRATORA SYSTEMU INFORMATYCZNEGO – WZÓR			Załącznik nr 4

. . . . . .

(miejscowość, data)

Powołanie
Administratora Systemu Informatycznego

Działając jako Administrator Danych, niniejszym, na mocy art. 24 ust. 1 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) dalej jako „RODO" z dniem . . . . . .

powołuję/wyznaczam

Panią/Pana* . . . . . .

na stanowisko Administratora Systemu Informatycznego

w . . . . . .

Zakres obowiązków oraz warunki pełnienia funkcji Administratora Systemu Informatycznego określone są 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), w ustawie o ochronie danych osobowych, w przepisach do niej wykonawczych oraz w dokumentacji ochrony danych osobowych Administratora w szczególności Polityce Ochrony Danych Osobowych, z treścią których Administrator Systemu Informatycznego ma obowiązek się zapoznać.

. . . . . .

(data i podpis Inspektora Ochrony Danych)

. . . . . .

(data i podpis osoby reprezentującej Administratora Danych)

Przyjmuję

. . . . . .

(data i podpis Administratora Systemów Informatycznych)

*niepotrzebne skreślić

Administrator Systemu Informatycznego (ASI) realizuje zadania w zakresie zarządzania i bieżącego nadzoru nad systemem informatycznym Administratora Danych (AD), w tym zwłaszcza odpowiedzialny jest za:

1. wdrożenie zasad ochrony danych osobowych określonych w Polityce Ochrony Danych Osobowych oraz Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych i dokumentach z nimi związanych;
2. realizację wytycznych Administratora Danych oraz Inspektora Ochrony Danych w zakresie ochrony danych osobowych przetwarzanych z wykorzystaniem środków informatycznych;
3. prowadzenie dokumentacji systemowej opisującej działania związane z administracją systemów informatycznych, w których przetwarzane są dane osobowe;
4. prowadzenie dokumentacji dotyczącej opisu przepływu danych pomiędzy systemami informatycznymi zastosowanymi w celu przetwarzania danych osobowych oraz udostępnianie jej Inspektorowi Ochrony Danych;
5. umożliwienie przeprowadzenia kontroli przez służby Prezesa Urzędu ochrony Danych Osobowych;
6. nadzór nad stosowaniem środków zapewniających bezpieczeństwo przetwarzania danych osobowych w systemach informatycznych, a w szczególności przeciwdziałających dostępowi osób niepowołanych do tych systemów;
7. zarządzanie systemem informatycznym, w którym przetwarzane są dane osobowe, posługując się hasłem administracyjnym dostępu do wszystkich stacji roboczych i serwerów z pozycji administratora;
8. nadzór nad prawidłowym działaniem mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych;
9. na wniosek Administratora Danych, zaopiniowany przez Inspektora Ochrony Danych, przydzielenie każdemu użytkownikowi identyfikatora oraz hasła do systemu informatycznego oraz dokonanie ewentualnych modyfikacji uprawnień, a także usuwanie kont użytkowników zgodnie z zasadami określonymi w Instrukcji (przydzielenie identyfikatora oraz hasła do systemu informatycznego może nastąpić wyłącznie w odniesieniu do osoby posiadającej upoważnienie do przetwarzania danych osobowych);
10. podejmowanie działań w zakresie ustalania i kontroli identyfikatorów dostępu do systemu informatycznego;
11. sprawowanie nadzoru nad bezpieczeństwem danych osobowych zawartych na dyskach wymiennych, palmtopach, pamięciach przenośnych i innych nośnikach, a także w komputerach przenośnych;
12. sprawowanie nadzoru nad systemem komunikacji w sieci publicznej poprzez terminale komputerowe Administratora Danych oraz przesyłanie danych za pośrednictwem urządzeń teletransmisji;
13. instalację i konfigurację oprogramowania systemowego i sieciowego zabezpieczającego dane chronione przed nieupoważnionym dostępem;
14. zarządzanie, sprawowanie nadzoru oraz serwis urządzeń komputerowych pracujących w systemie informatycznym, w tym świadczenie pomocy technicznej dla użytkowników;
15. w sytuacji stwierdzenia naruszenia zabezpieczeń systemu informatycznego alarmowanie Administratora Danych oraz Inspektora Ochrony Danych o naruszeniu oraz współdziałanie z nimi przy usuwaniu skutków naruszenia;
16. zarządzanie kopiami awaryjnymi konfiguracji oprogramowania systemowego i sieciowego;

17. zarządzanie kopiami awaryjnymi danych oraz zasobów umożliwiających ich przetwarzanie;
18. zapewnianie bieżącego monitoringu, ciągłości działania oraz optymalizacji wydajności systemu informatycznego;
19. diagnozowanie zdarzeń i usuwanie awarii urządzeń komputerowych;
20. wykonywanie oraz sprawowanie nadzoru nad wykonywaniem napraw, konserwacją oraz likwidacją urządzeń komputerowych, na których przetwarzane są dane osobowe;
21. wykonywanie oraz sprawowanie nadzoru nad wykonywaniem kopii zapasowych, ich przechowywaniem oraz okresowym sprawdzaniem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu informatycznego;
22. podejmowanie działań służących zapewnieniu niezawodności zasilania komputerów, innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz zapewnieniu bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej teletransmisji;
23. identyfikowanie i analizowanie zagrożeń, w tym dokonywanie ocen ryzyka, na które może być narażone przetwarzanie danych osobowych w systemach informatycznych;
24. prowadzenie ewidencji sprzętu i oprogramowania;
25. opiniowanie i wnioskowanie zakupów urządzeń komputerowych, urządzeń sieciowych i serwerowych, oprogramowania komputerowego, sieciowego i serwerowego;
26. instalowanie albo nadzór nad instalacją nowo kupionych urządzeń komputerowych;
27. wprowadzanie zmiany w konfiguracji lokalnych urządzeń komputerowych, lokalnym oprogramowaniu systemowym oraz aplikacyjnym po uzgodnieniu z Inspektorem Ochrony Danych;
28. konfigurację i administrowanie oprogramowaniem systemowym na stacjach roboczych, archiwizowanie danych z lokalnych stacji roboczych;
29. współpracę z dostawcami usług, sprzętu sieciowego i serwerowego oraz zapewnienie przestrzegania przepisów dotyczących ochrony danych osobowych;
30. wnioskowanie do Administratora Danych o wprowadzenie zmian w procedurach bezpieczeństwa i standardach zabezpieczeń.

	INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH	Wersja	1.00
		Data opracowania	……..
		Właściciel	……..
ANULOWANIE POWOŁANIA ADMINISTRATORA SYSTEMU INFORMATYCZNEGO – WZÓR			Załącznik nr 5

. . . . . .

(miejscowość, data)

Anulowanie Powołania
Administratora Systemu Informatycznego

Działając jako Administrator Danych, niniejszym z dniem . . . . . .
anuluję powołanie/wyznaczenia Pani/Pana*

. . . . . .

na stanowisko Administratora Systemu Informatycznego w . . . . . .

. . . . . .

(data i podpis osoby reprezentującej Administratora Danych)

Potwierdzam

. . . . . .

(data i podpis Administrator Systemu Informatycznego)

*niepotrzebne skreślić

	INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH	Wersja	1.00
		Data opracowania	……..
		Właściciel	……..
OŚWIADCZENIE ADMINISTRATORA SYSTEMU INFORMATYCZNEGO – WZÓR			Załącznik nr 6

. . . . . .

(miejscowość, data)

Oświadczenie Administratora Systemu Informatycznego

Ja niżej podpisany . . . . . .

zam. . . . . ,

Nr Pesel: . . . . . , oświadczam, iż

1. posiadam kwalifikacje zawodowe, a w szczególności fachową wiedzę na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętność wypełnienia powierzonych mi zadań Administratora Systemu Informatycznego;
2. zobowiązuję się do niezwłocznego poinformowania Administratora Danych o zmianie okoliczności objętych niniejszym oświadczeniem;
3. zobowiązuje się wypełniać z należytą starannością oraz z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania, m.in. następujące zadania:
   a) wdrożenie zasad ochrony danych osobowych określonych w Polityce Ochrony Danych Osobowych oraz Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych i dokumentach z nimi związanych;
   b) realizację wytycznych Administratora Danych oraz Inspektora Ochrony Danych w zakresie ochrony danych osobowych przetwarzanych z wykorzystaniem środków informatycznych;
   c) prowadzenie dokumentacji systemowej opisującej działania związane z administracją systemów informatycznych, w których przetwarzane są dane osobowe;
   d) prowadzenie dokumentacji dotyczącej opisu przepływu danych pomiędzy systemami informatycznymi zastosowanymi w celu przetwarzania danych osobowych oraz udostępnianie jej Inspektorowi Ochrony Danych;
   e) umożliwienie przeprowadzenia kontroli przez służby Prezesa Ochrony Danych Osobowych;
   f) nadzór nad stosowaniem środków zapewniających bezpieczeństwo przetwarzania danych osobowych w systemach informatycznych, a w szczególności przeciwdziałających dostępowi osób niepowołanych do tych systemów;
   g) zarządzanie systemem informatycznym, w którym przetwarzane są dane osobowe, posługując się hasłem administracyjnym dostępu do wszystkich stacji roboczych i serwerów z pozycji administratora;
   h) nadzór nad prawidłowym działaniem mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych;

i) na wniosek Administratora Danych, przydzielenie każdemu użytkownikowi identyfikatora oraz hasła do systemu informatycznego oraz dokonanie ewentualnych modyfikacji uprawnień, a także usuwanie kont użytkowników zgodnie z zasadami określonymi w Instrukcji (przydzielenie identyfikatora oraz hasła do systemu informatycznego może nastąpić wyłącznie w odniesieniu do osoby posiadającej upoważnienie do przetwarzania danych osobowych);
j) podejmowanie działań w zakresie ustalania i kontroli identyfikatorów dostępu do systemu informatycznego;
k) sprawowanie nadzoru nad bezpieczeństwem danych osobowych zawartych na dyskach wymiennych, palmtopach, pamięciach przenośnych i innych nośnikach, a także w komputerach przenośnych;
l) sprawowanie nadzoru nad systemem komunikacji w sieci publicznej poprzez terminale komputerowe Administratora Danych oraz przesyłanie danych za pośrednictwem urządzeń teletransmisji;
m) instalację i konfigurację oprogramowania systemowego i sieciowego zabezpieczającego dane chronione przed nieupoważnionym dostępem;
n) zarządzanie, sprawowanie nadzoru oraz serwis urządzeń komputerowych pracujących w systemie informatycznym, w tym świadczenie pomocy technicznej dla użytkowników;
o) w sytuacji stwierdzenia naruszenia zabezpieczeń systemu informatycznego alarmowanie Administratora Danych oraz Inspektora Ochrony Danych o naruszeniu oraz współdziałanie z nimi przy usuwaniu skutków naruszenia;
p) zarządzanie kopiami awaryjnymi konfiguracji oprogramowania systemowego i sieciowego;
q) zarządzanie kopiami awaryjnymi danych (w tym danych osobowych) oraz zasobów umożliwiających ich przetwarzanie;
r) zapewnianie bieżącego monitoringu, ciągłości działania oraz optymalizacji wydajności systemu informatycznego;
s) diagnozowanie zdarzeń i usuwanie awarii urządzeń komputerowych;
t) wykonywanie oraz sprawowanie nadzoru nad wykonywaniem napraw, konserwacją oraz likwidacją urządzeń komputerowych, na których przetwarzane są dane osobowe;
u) wykonywanie oraz sprawowanie nadzoru nad wykonywaniem kopii zapasowych, ich przechowywaniem oraz okresowym sprawdzaniem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu informatycznego;
v) podejmowanie działań służących zapewnieniu niezawodności zasilania komputerów, innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz zapewnieniu bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej teletransmisji;
w) identyfikowanie i analizowanie zagrożeń, w tym dokonywanie ocen ryzyka, na które może być narażone przetwarzanie danych osobowych w systemach informatycznych;
x) prowadzenie ewidencji sprzętu i oprogramowania;
y) opiniowanie i wnioskowanie zakupów urządzeń komputerowych, urządzeń sieciowych i serwerowych, oprogramowania komputerowego, sieciowego i serwerowego;
z) instalowanie albo nadzór nad instalacją nowo kupionych urządzeń komputerowych;

aa) wprowadzanie zmiany w konfiguracji lokalnych urządzeń komputerowych, lokalnym oprogramowaniu systemowym oraz aplikacyjnym po uzgodnieniu z Inspektorem Ochrony Danych;

ab) konfigurację i administrowanie oprogramowaniem systemowym na stacjach roboczych, archiwizowanie danych z lokalnych stacji roboczych;

ac) współpracę z dostawcami usług, sprzętu sieciowego i serwerowego oraz zapewnienie przestrzegania przepisów dotyczących ochrony danych osobowych;

ad) wnioskowanie do Administratora Danych o wprowadzenie zmian w procedurach bezpieczeństwa i standardach zabezpieczeń.

. . . . . .

(data i podpis Administratora Systemu Informatycznego)

Przyjmuje oświadczenie

. . . . . .

(data i podpis osoby reprezentującej Administratora Danych)

*niepotrzebne skreślić

	INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH	Wersja	1.00
		Data opracowania	……...
		Właściciel	……...
REJESTR MOBLINYCH NOŚNIKÓW DANYCH – WZÓR			Załącznik nr 7

. . . . . .

(miejscowość, data)

Rejestr mobilnych nośników pamięci używanych do przetwarzania danych

Lp.	Oznaczenie nośnika	Data wpisania do rejestru	Opis nośnika	Miejsce przechowywania nośnika	Podpis użytkownika	Uwagi
1.						
2.						
3.						
4.						
5.						
6.						
7.						

. . . . . .

Administrator Systemu Informatycznego

(miejsce, data, podpis)

	INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH	Wersja	1.00
		Data opracowania	……..
		Właściciel	……..
REJESTR INCYDENTÓW INFORMATYCZNYCH – WZÓR			Załącznik nr 8

. . . . . .

(miejscowość, data)

Rejestr incydentów informatycznych

Lp.	Kategoria	Opis
1.	Data i godzina incydentu	
2.	Miejsce incydentu	
3.	System / Podsystem / Aplikacja	
4.	Dane osoby zgłaszającej (imię i nazwisko, komórka organizacyjna)	
5.	Charakter zdarzenia	Nieuprawniony dostęp do systemu – tak / nie
		Nieuprawniony dostęp do danych – tak / nie
		Nieuprawniony przekaz danych – tak / nie
		Kradzież danych – tak / nie
		Utrata danych – tak / nie
		Wykrycie wirusa – tak / nie
		Mechaniczne uszkodzenie urządzeń – tak / nie
		Inne (podać jakie)
6.	Dane świadka zdarzenia (imię i nazwisko, komórka organizacyjna)	

Dokładny opis incydentu

. . . . . .
. . . . . .
. . . . . .

Podjęte środki naprawcze

. . . . . .
. . . . . .
. . . . . .

Wnioski

. . . . . .
. . . . . .
. . . . . .

Lp.	Numer raportu z incydentu	Data i godzina incydentu	Imię i nazwisko osoby zgłaszającej (komórka organizacyjna / numer pomieszczenia)	System informatyczny / Podsystem / Aplikacja	Opis incydentu	Uwagi Podpis ASI
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						
9.						
10.						

. . . . . .

Administrator Systemu Informatycznego

(miejsce, data, podpis)

	INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH	Wersja	1.00
		Data opracowania	……..
		Właściciel	……..
OŚWIADCZENIE – SZKOLENIE INFORMATYCZNE – WZÓR			Załącznik nr 9

. . . . . .

(miejscowość, data)

Oświadczenie o wzięciu udziału w szkoleniu w zakresie wykonywanych zadań w Systemie Informatycznym oraz zobowiązaniu się do przestrzegania przedstawionych w trakcie szkolenia zasad ochrony danych osobowych

Ja niżej podpisany** . . . . . ,
zam. . . . . ,
Nr Pesel: . . . . . ,
oświadczam, iż w dniu . . . . . został*am/został*em zapoznana/zapoznany*,
przeszkolony(a) i przeszedł*em(am) instruktaż w zakresie obsługi niżej wymienionych modułów Systemu Informatycznego
. . . . . :

- moduł . . . . . .
- moduł . . . . . .
- moduł . . . . . .
- inne uprawnienia . . . . . .

Jednocześnie oświadczam, iż jestem upoważniony do przetwarzania danych osobowych w zbiorach danych osobowych Administratora Danych w następujących Systemach Informatycznych:

Lp.	Nazwa procesu	Forma przetwarzania	Nazwa systemu informatycznego
1.		informatyczna	
2.		informatyczna	
3.		informatyczna	
4.		informatyczna	
5.		informatyczna	
6.		informatyczna	

Zobowiązuję się do:

a) zachowania w tajemnicy danych osobowych przetwarzanych przez Administratora Danych,
b) zachowania w tajemnicy sposobu zabezpieczenia i przetwarzania danych osobowych przetwarzanych u Administratora Danych,

c) nieujawniania danych osobowych podmiotom nieuprawnionym w jakiejkolwiek formie bez zgody Administratora Danych,
d) przestrzegania Polityki Ochrony Danych Osobowych oraz Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych,
e) korzystania z oprogramowania Administratora Danych wyłącznie w związku z wykonywaniem obowiązków pracowniczych,
f) wykorzystywania jedynie legalnego oprogramowania pochodzącego od Administratora Danych,
g) niepodejmowania prób samodzielnego instalowania oprogramowania pochodzącego z innych źródeł,
h) wnoszenia, wynoszenia i użytkowania komputerów przenośnych bądź innych nośników danych wyłącznie za wiedzą i zgodą Inspektora Ochrony Danych lub Administratora Systemu Informatycznego,
i) należytej dbałości o sprzęt i oprogramowanie,
j) należytego zabezpieczania dokumentów papierowych przed nieuprawnionym dostępem, uszkodzeniem lub zniszczeniem,
k) należytego zabezpieczania pomieszczeń, w których przetwarza się dane osobowe.

Naruszenie przez osobę upoważnioną jej podstawowych obowiązków w zakresie wskazanym powyżej, będzie stanowić podstawę do podjęcia przez Administratora Danych przysługujących mu środków prawnych, a w szczególności może stanowić przyczynę uzasadniającą wypowiedzenie przez Administratora Danych umowy lub rozwiązanie tejże umowy bez wypowiedzenia, z winy naruszającego. Naruszenie zasad ochrony danych osobowych może spowodować odpowiedzialność karną, jak również odpowiedzialność odszkodowawczą na zasadach określonych w przepisach prawa powszechnie obowiązującego.

. . . . . .

(data i podpis osoby przeszkolonej)

* niepotrzebne skreślić

** dotyczy w szczególności pracowników, przedsiębiorców, stażystów, praktykantów, wolontariuszy itp.

Potwierdzam

. . . . . .

Administrator Systemu Informatycznego

(miejsce, data, podpis)

	INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH	Wersja	1.00
		Data opracowania	……...
		Właściciel	……...
DZIENNIK ADMINISTRATORA SYSTEMU INFORMATYCZNEGO – WZÓR			Załącznik nr 10

. . . . . .

(miejscowość, data)

Dziennik
Administratora Systemu Informatycznego

Lp.	System informatyczny / Podsystem / Aplikacja	Wykonane sprawdzenia bezpieczeństwa teleinformatycznego	Wykonane audyty bezpieczeństwa teleinformatycznego	Wykonane kontrole bezpieczeństwa teleinformatycznego	Wnioski	Uwagi / Podpis ASI
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						
9.						

. . . . . .

Administrator Systemu Informatycznego

(miejsce, data, podpis)

ZAŁĄCZNIKI

MONITOR POLSKI

DZIENNIK URZĘDOWY RZECZYPOSPOLITEJ POLSKIEJ

Warszawa, dnia 8 lipca 2019 r.

Poz. 666

KOMUNIKAT
PREZESA URZĘDU OCHRONY DANYCH OSOBOWYCH

z dnia 17 czerwca 2019 r.

w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony

Na podstawie art. 54 ust. 1 pkt 1 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. poz. 1000 i 1669 oraz z 2019 r. poz. 730) w związku z art. 35 ust. 4 i 6 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) (Dz. Urz. UE L 119 z 04.05.2016, str. 1 oraz L 127 z 23.05.2018, str. 2) ogłasza się, co następuje:

1) ogłasza się wykaz rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony, o którym mowa w art. 35 ust. 4 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) – wykaz określa załącznik do komunikatu;

2) wykaz, o którym mowa w pkt 1, uchyla zawarty w komunikacie Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 sierpnia 2018 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony (M.P. poz. 827), wykaz nieobejmujący czynności przetwarzania związanych z oferowaniem towarów lub usług osobom, których dane dotyczą, lub z monitorowaniem ich zachowania w kilku państwach członkowskich Unii Europejskiej.

Prezes Urzędu Ochrony Danych Osobowych: *J. Nowak*

Załącznik do komunikatu Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 czerwca 2019 r. (poz. 666)

WYKAZ RODZAJÓW OPERACJI PRZETWARZANIA DANYCH OSOBOWYCH WYMAGAJĄCYCH PRZEPROWADZENIA OCENY SKUTKÓW PRZETWARZANIA DLA ICH OCHRONY

Poniższy wykaz zawiera rodzaje operacji przetwarzania, które w opinii Urzędu Ochrony Danych Osobowych wymagają oceny skutków dla ochrony danych. Wykaz ten został opracowany w ramach realizacji obowiązku nałożonego na Urząd Ochrony Danych Osobowych na podstawie art. 35 ust. 4 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) jako polski organ nadzorczy. Wykaz ten nie zwalnia administratora z obowiązku przeanalizowania wszelkich operacji przetwarzania danych w oparciu o pełną ocenę skutków dla ochrony danych na podstawie art. 35 ust. 1 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). Wykaz został opracowany w oparciu o wytyczne Grupy Roboczej Artykułu 29 (WP 248) „Wytyczne dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie «może powodować wysokie ryzyko» do celów rozporządzenia 2016/679". Wykaz ten uzupełnia i konkretyzuje powyższe wytyczne.

Co do zasady, przetwarzanie spełniające przynajmniej dwa z niżej wymienionych kryteriów będzie wymagać oceny skutków dla ochrony danych. W niektórych przypadkach administrator danych może jednak uznać, że przetwarzanie spełniające tylko jedno z niżej wymienionych kryteriów będzie wymagało przeprowadzenia oceny skutków dla ochrony danych. Im więcej kryteriów spełnia przetwarzanie, tym bardziej prawdopodobne jest wystąpienie wysokiego ryzyka naruszenia praw lub wolności podmiotów danych, a w konsekwencji, niezależnie od środków przewidzianych przez administratora do zastosowania, wymagana będzie ocena skutków dla ochrony danych.

Urząd Ochrony Danych Osobowych podkreśla, że każdy z przykładów obszarów zastosowania ma charakter wyłącznie ilustracyjny, a w konsekwencji „Przykłady operacji/ zakresu danych/ okoliczności, w których może wystąpić wysokie ryzyko naruszenia dla danego rodzaju operacji przetwarzania" nie mają charakteru wyczerpującego. Zawarte w wykazie przykłady mają jedynie na celu pomoc w lepszym zrozumieniu kryteriów/rodzajów operacji mogących skutkować koniecznością przeprowadzenia oceny skutków dla ochrony danych.

Wykaz ten w żaden sposób nie narusza ogólnego obowiązku administratora do dokonania właściwej oceny ryzyka i zarządzania ryzykiem. Przeprowadzenie oceny skutków dla ochrony danych nie zwalnia również administratora z innych obowiązków 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) oraz z obowiązków określonych w innych właściwych przepisach.

I. Rodzaje/kryteria dla operacji przetwarzania, dla których wymagane jest przeprowadzenie oceny	**II. Potencjalne obszary wystąpienia/ istniejące obszary zastosowań**	**III. Przykłady operacji/zakresu danych/okoliczności, w których może wystąpić wysokie ryzyko naruszenia dla danego rodzaju operacji przetwarzania**
1. Ewaluacja lub ocena, w tym profilowanie i przewidywanie (analiza behawioralna) w celach wywołujących negatywne skutki prawne, fizyczne, finansowe lub inne niedogodności dla osób fizycznych	Media społecznościowe, firmy marketingowe, firmy headhunterskie	Profilowanie użytkowników portali społecznościowych i innych aplikacji w celu wysyłania informacji handlowej
	Banki, inne instytucje finansowe upoważnione do udzielania kredytów, instytucje pożyczkowe w procesie oceny zdolności kredytowej	Ocena zdolności kredytowej, przy użyciu algorytmów sztucznej inteligencji, objęta obowiązkiem zachowania tajemnicy i żądanie ujawnienia danych niemających bezpośredniego związku z oceną zdolności kredytowej
	Firmy ubezpieczeniowe – oferowanie zniżek związanych ze stylem życia (papierosy, alkohol, sporty ekstremalne, styl jazdy samochodem)	Ocena stylu życia, odżywiania się, jazdy, sposobu spędzania czasu itp. osób fizycznych w celu np. podwyższenia im ceny składki ubezpieczeniowej, na podstawie tej oceny, nazywana ogólnie optymalizacją składki ubezpieczeniowej

	Firmy ubezpieczeniowe – np. korzystniejsze oferty ubezpieczeniowe lub kredytowe dla pracowników określonych grup, np. administracji publicznej, nauczycieli	Profilowanie pośrednie (ocena osoby na podstawie przynależności do określonej grupy)
2. Zautomatyzowane podejmowanie decyzji wywołujących skutki prawne, finansowe lub podobne istotne skutki	Drogi objęte odcinkowym pomiarem prędkości (system gromadzi informacje nie tylko o pojazdach naruszających przepisy, ale o wszystkich pojazdach pojawiających się w kontrolowanym obszarze), odcinki dróg wyposażone w system elektronicznego poboru opłat viaTOLL	Systemy monitoringu wykorzystywane do zarządzania ruchem, umożliwiające szczegółowy nadzór nad kierowcą oraz jego zachowaniem na drodze, w szczególności systemy pozwalające na automatyczną identyfikację pojazdów Systemy automatycznego pobierania opłat za wjazd
	Sklepy internetowe oferujące ceny promocyjne dla określonych grup klientów. Firmy obsługujące programy lojalnościowe (wspólnoty zakupowe)	Systemy profilowania klientów pod kątem zidentyfikowania preferencji zakupowych, automatycznego ustalania cen promocyjnych w oparciu o profil
	Programy marketingowe zawierające elementy profilowania osób	Monitorowanie zakupów i preferencji zakupowych (np. alkohol, słodycze)
3. Systematyczne monitorowanie na dużą skalę miejsc dostępnych publicznie wykorzystujące elementy rozpoznawania cech lub właściwości obiektów, które znajdą się w monitorowanej przestrzeni. Do tej grupy systemów nie są zaliczane systemy monitoringu wizyjnego, w których obraz jest nagrywany i wykorzystywany tylko w przypadku potrzeby analizy incydentów naruszenia prawa	Środki komunikacji miejskiej, miasta oferujące systemy wypożyczania rowerów, samochodów oraz wyznaczające strefy płatnego parkowania	Monitorowanie osób korzystających z usług w przestrzeni publicznej, przy wykorzystaniu danych wykraczających poza dane niezbędne do świadczenia tych usług
	Zakłady pracy (monitoring systemów informatycznych poczty elektronicznej, używanego oprogramowania, kart dostępowych itp.)	Systemy monitorowania czasu pracy pracowników oraz przepływu informacji w wykorzystywanych przez nich narzędziach (poczty elektronicznej, Internetu) Kryterium: systematyczne monitorowanie (*vide* WP 249[1]) + wrażliwe podmioty danych
	Przetwarzanie informacji pozyskiwanych przez Internet rzeczy (opaski medyczne, smartwatche itp.) oraz ich przesyłanie w sieci przy użyciu urządzeń mobilnych typu smartfon czy tablet	Gromadzenie i wykorzystywanie danych przez aplikacje instalowane w urządzeniach mobilnych, w tym w urządzeniach zintegrowanych z mundurem, kaskiem lub w inny sposób połączonych z osobą pozyskującą dane
	Systemy komunikujące się typu maszyna – maszyna, w których samochód informuje otoczenie o swoim zachowaniu (ruchu) i w przypadku pojawiającego się zagrożenia otrzymuje od tego otoczenia (infrastruktura drogowa, inne samochody) komunikaty ostrzegawcze	Systemy monitoringu pojazdów nawiązujące połączenia z otoczeniem, w tym z innymi pojazdami
	Opinia Europejskiego Komitetu Ekonomiczno-Społecznego w sprawie identyfikacji radiowej (RFID) (2007/C 256/13)	Systemy wykorzystujące RFID w przypadku, gdy znaczniki/etykiety są lub mogą być przypisane osobom fizycznym
	Szpitale/Organizacje prowadzące badania kliniczne. Kluby fitness/ podmioty/ organizacje pobierające materiał genetyczny do badań	Dane dotyczące zdrowia pacjentów/klientów
4. Przetwarzanie szczególnych kategorii danych osobowych i dotyczących wyroków skazujących i czynów zabronionych (danych wrażliwych wg opinii WP 29)	Partie polityczne, komitety wyborcze, komitety referendalne i inicjatywy ustawodawcze, organizacje społeczne, kampanie wyborcze	Przetwarzanie przez organy państwowe lub podmioty prywatne danych osobowych dotyczących przynależności partyjnej i/lub preferencji wyborczych
	Operatorzy telekomunikacyjni; dostawcy mediów (prąd, gaz, woda) w zakresie inteligentnego opomiarowania – Zalecenie 2012/148/UE Komisji Europejskiej z marca 2012 r. w sprawie przygotowań do rozpowszechniania inteligentnych systemów pomiarowych	Regularne przetwarzanie danych pomiarowych umożliwiające obserwację stylu życia, przemieszczania się w terenie, intensywności korzystania z mediów, energii itp. (np. danych geolokalizacyjnych, danych z inteligentnych liczników pomiarowych o zużywanej energii, danych bilingowych dotyczących komunikacji elektronicznej itp.)

[1] Opinia 2/2017 na temat przetwarzania danych w miejscu pracy (08.06.2017).

	Usługi poczty elektronicznej; systemy monitoringu osiągnięć sportowych współpracujące z opaskami typu fitness wykorzystujące chmurę obliczeniową; aplikacje dostarczane przez producentów czytników elektronicznych do zakupu książek, gazet elektronicznych z funkcjami robienia notatek itp.	Serwisy internetowe i inne systemy informatyczne oferowane osobom fizycznym do przetwarzania informacji obejmujących działania o charakterze czysto osobistym lub domowym (jak np. usługi przetwarzania w chmurze do zarządzania dokumentami osobistymi, usługi poczty elektronicznej, kalendarze, e-czytniki wyposażone w funkcje robienia notatek oraz różne aplikacje typu „life-logging", które mogą zawierać informacje o bardzo osobistym charakterze), których ujawnienie lub przetwarzanie do celów innych niż czynności o charakterze domowym może być uznane za bardzo ingerujące w prywatność
5. Przetwarzanie danych biometrycznych wyłącznie w celu identyfikacji osoby fizycznej bądź w celu kontroli dostępu	Systemy rozpoznawania twarzy, weryfikacja tożsamości w miejscu pracy w celu kontroli dostępu, weryfikacja tożsamości w urządzeniach/ aplikacjach (wliczając rozpoznawanie głosu, odcisków palców, twarzy); systemy monitoringu wejść do określonych pomieszczeń; systemy rozliczeniowo--ewidencyjne operacji bankowych, handlowych, ubezpieczeniowych; systemy kontroli wejść do klubów fitness, hoteli itp.	Wejścia do określonych obszarów, pomieszczeń lub uzyskanie dostępu do określonego konta w systemie informatycznym w celu np. wykonania zlecenia transakcji w systemie teleinformatycznym lub wypłaty gotówki przy użyciu bankomatu itp.
6. Przetwarzanie danych genetycznych	Laboratoria/Firmy/Szpitale oferujące diagnostykę genetyczną	Diagnoza medyczna Testy DNA Badania medyczne
7. Dane przetwarzane na dużą skalę, gdzie pojęcie dużej skali dotyczy: **• liczby osób, których dane są przetwarzane,** **• zakresu przetwarzania,** **• okresu przechowywania danych oraz** **• geograficznego zakresu przetwarzania**	Centralny system: – informacji oświatowej; – informacji w szkolnictwie wyższym; – obsługi ubezpieczeń komunikacyjnych; – kwalifikacji zawodowych itp.	Centralne zbiory danych wspomagające zarządzanie określoną grupą osób w celach związanych z realizacją zadań publicznych, z których dane udostępniane są w różnym zakresie w zależności od ich roli i zadań związanych z realizacją tych obowiązków
	Portale społecznościowe, przeglądarki internetowe, dostawcy usług telewizji kablowej, serwisy subskrypcyjne z filmami i programami telewizyjnymi dostępne na urządzeniach z dostępem do Internetu	Zbieranie szerokiego zakresu danych o przeglądanych stronach internetowych, realizowanych zakupach/ historii zakupów, oglądanych programach telewizyjnych lub radiowych itp.
8. Przeprowadzanie porównań, ocena lub wnioskowanie na podstawie analizy danych pozyskanych z różnych źródeł	Firmy marketingowe pobierające dane z różnych źródeł, gdzie występują dane osobowe o klientach, w celach przeprowadzania ukierunkowanych na określone grupy klientów akcji marketingowych	Łączenie danych z różnych rejestrów państwowych i/lub publicznych
	Firmy marketingowe w celach doskonalenia i rozszerzania profili potencjalnych klientów oraz doskonalenia usług reklamy ukierunkowanej na określone usług reklamy ukierunkowanej na określone grupy społeczne; firmy obsługujące programy lojalnościowe (wspólnoty zakupowe)	Tworzenie profili osób ze zbiorów danych pochodzących z różnych źródeł (łączenie zbiorów)
	Portale społecznościowe, sieci handlowe, firmy marketingowe, banki i instytucje finansowe	Zbieranie danych o przeglądanych stronach, wykonywanych operacjach bankowych, zakupach w sklepach internetowych, a następnie ich analiza w celu tworzenia profilu osoby
9. Przetwarzanie danych dotyczących osób, których ocena i świadczone im usługi są uzależnione od podmiotów lub osób, które dysponują uprawnieniami nadzorczymi i/lub ocennymi	Serwisy oferujące pracę, które dokonują dopasowania ofert do określonych preferencji pracodawców	Przetwarzanie danych, w których dokonuje się klasyfikacji lub ocen osób, których dane dotyczą, pod względem np. wieku, płci, a następnie klasyfikacje te wykorzystuje się do przedstawienia ofert lub innych działań, które mogą mieć wpływ na prawa lub wolność osób, których dane są przetwarzane
	Systemy służące do zgłaszania nieprawidłowości (whistleblowing)	Systemy służące do zgłaszania nieprawidłowości (związanych np. z korupcją, mobbingiem) – w szczególności gdy przetwarzane są w nim dane pracowników

10. Innowacyjne wykorzystanie lub zastosowanie rozwiązań technologicznych lub organizacyjnych	Sprzedawcy i dystrybutorzy mediów (prąd, gaz, woda, usługi telekomunikacyjne) wdrażający inteligentne liczniki	Systemy zdalnego opomiarowania, które, biorąc pod uwagę zakres i częstość zbierania danych, umożliwiają profilowanie osób lub grupy osób
	Serwisy internetowe przetwarzające dane z urządzeń typu Internet rzeczy, np. aparatów fotograficznych wyposażonych w funkcje lokalizacyjne (GPS)	Systemy analizy i przetwarzania danych znajdujących się w metadanych, np. zdjęcia opatrzone danymi geolokalizacyjnymi
	Zastosowanie komunikacji między urządzeniami (Internet rzeczy – np. beacony, drony) w przestrzeni publicznej i w miejscach użyteczności publicznej	Systemy stosowane do analizy i przekazywania danych dostawcom usługi przy użyciu aplikacji mobilnych z urządzeń przenośnych typu: smartwatch, inteligentne opaski, beacony itp. analizujące i przekazujące dane dostawcom przy użyciu aplikacji mobilnych
	Aplikacje z funkcjami komunikowania się i oprogramowaniem umożliwiającym wymianę informacji z najbliższym otoczeniem oraz zdalnie poprzez sieć telekomunikacyjną	Stosowanie urządzeń wyposażonych w różnego rodzaju interfejsy (głośnik, mikrofon, kamera) oraz oprogramowanie i system łączności umożliwiające przekazywanie danych poprzez sieci telekomunikacyjne
	Zabawki interaktywne	Usługi i zabawki dedykowane dzieciom
	Specjalistyczne porady i konsultacje medyczne, badania kliniczne o zasięgu międzynarodowym	Konsultacje telemedyczne z ośrodkami spoza UE, przekazywanie osobowych danych medycznych o zasięgu międzynarodowym
11. Gdy przetwarzanie samo w sobie uniemożliwia osobom, których dane dotyczą, wykonywanie prawa lub korzystanie z usługi lub umowy	Podmioty udzielające pożyczek i kredytów oraz oferujące sprzedaż ratalną	Podejmowanie decyzji kredytowej w stosunku do potencjalnych klientów na podstawie informacji zawartych w bazach zawierających informacje o dłużnikach lub podobnych bazach danych
	Sklepy internetowe oraz dostawcy innych usług typu gry, muzyka, loterie itp.	Uzależnianie możliwości korzystania z usługi od informacji w zakresie dochodów, kwoty wydatków miesięcznych i innych wartości zebranych w wyniku profilowania
12. Przetwarzanie danych lokalizacyjnych	Urządzenia, aplikacje i platformy wykorzystujące Internet rzeczy. Przetwarzanie danych w kontekście pracy w domu i pracy wykonywanej zdalnie. Przetwarzanie danych lokalizacyjnych pracowników	Przetwarzanie wykorzystujące śledzenie lokalizacji osoby fizycznej (wliczając sieci komunikacyjne i usługi komunikacyjne, wskazujące geograficzną pozycję telekomunikacyjnych terminali urządzeń użytkownika publicznie dostępnej usługi telekomunikacyjnej)

Zawiadomienie o wyznaczeniu nowego inspektora ochrony danych

Część A: Oznaczenie administratora danych/podmiotu przetwarzającego

Pełna nazwa administratora/podmiotu przetwarzającego	Kliknij tutaj, aby wprowadzić tekst.	
REGON (jeśli został nadany) (opcjonalnie)	Kliknij tutaj, aby wprowadzić tekst.	
Sektor (opcjonalnie)	*Dla sektora publicznego:* Wybierz element.	*Dla sektora prywatnego:* Wybierz element.

Adres:

Państwo	Kliknij tutaj, aby wprowadzić tekst.	Miejscowość	Kliknij tutaj, aby wprowadzić tekst.
Województwo	Kliknij tutaj, aby wprowadzić tekst.	Ulica	Kliknij tutaj, aby wprowadzić tekst.
Powiat	Kliknij tutaj, aby wprowadzić tekst.	Kod pocztowy	Kliknij tutaj, aby wprowadzić tekst.
Gmina	Kliknij tutaj, aby wprowadzić tekst.	Numer domu	Podaj numer
		Numer lokalu	Podaj numer

Osoba/osoby uprawnione do reprezentowania administratora/podmiotu przetwarzającego

1.	Imię i nazwisko: Kliknij tutaj, aby wprowadzić tekst.	Stanowisko: Kliknij tutaj, aby wprowadzić tekst.
2.	Imię i nazwisko: Kliknij tutaj, aby wprowadzić tekst. (opcjonalnie)	Stanowisko: Kliknij tutaj, aby wprowadzić tekst. (opcjonalnie)
3.	Imię i nazwisko: Kliknij tutaj, aby wprowadzić tekst. (opcjonalnie)	Stanowisko: Kliknij tutaj, aby wprowadzić tekst. (opcjonalnie)
4.	Imię i nazwisko: Kliknij tutaj, aby wprowadzić tekst. (opcjonalnie)	Stanowisko: Kliknij tutaj, aby wprowadzić tekst. (opcjonalnie)
5.	Imię i nazwisko: Kliknij tutaj, aby wprowadzić tekst. (opcjonalnie)	Stanowisko: Kliknij tutaj, aby wprowadzić tekst. (opcjonalnie)

Część B: Dane kontaktowe inspektora ochrony danych

Imię	Kliknij tutaj, aby wprowadzić tekst.	Nazwisko	Kliknij tutaj, aby wprowadzić tekst.
Telefon	Kliknij tutaj, aby wprowadzić tekst.	Adres e-mail	Kliknij tutaj, aby wprowadzić tekst.

Powyżej musi zostać podany telefon lub adres e-mail (oba pola nie mogą pozostać puste – zgodnie z brzmieniem art. 10 ust. 1 ustawy o ochronie danych osobowych)

☐ Wniosek wypełniany przez pełnomocnika (opcjonalnie)

Pełnomocnictwo udzielone w formie elektronicznej oraz dowód uiszczenia opłaty skarbowej należy załączyć podczas składania wniosku przez portal biznes.gov.pl.
Pełnomocnictwo opatrzone kwalifikowanym podpisem elektronicznym osoby udzielającej pełnomocnictwa.

Administrator danych osobowych.
Administratorem Państwa danych osobowych będzie Prezes Urzędu Ochrony Danych Osobowych (Prezes UODO) z siedzibą w Warszawie, przy ul. Stawki 2.

Można się z nami kontaktować w następujący sposób:
a) listownie: ul. Stawki 2, 00-193 Warszawa
b) przez elektroniczną skrzynkę podawczą dostępną na stronie: https://www.uodo.gov.pl/pl/p/kontakt
c) telefonicznie: (22) 531 03 00

Inspektor ochrony danych.
Możecie się Państwo kontaktować również z wyznaczonym przez Prezesa UODO inspektorem ochrony danych pod adresem email IOD@uodo.gov.pl

Cele i podstawy przetwarzania.
Będziemy przetwarzać Państwa dane osobowe zawarte w formularzu w celu przyjmowania powiadomień o danych kontaktowych inspektora ochrony danych zgodnie z art. 37 ust. 7 RODO[1], a następnie dla wypełnienia obowiązku archiwizacji dokumentów wynikającego z ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach.

Odbiorcy danych osobowych.
Odbiorcami Państwa danych osobowych mogą być Minister Cyfryzacji w przypadku jeśli zawiadomienie do Prezesa UODO zostało wysłane przez platformę ePUAP i, dodatkowo, Minister Przedsiębiorczości i Technologii jeśli korespondencja do Prezesa UODO przesłana została drogą elektroniczną za pośrednictwem formularzy zamieszczonych na platformie biznes.gov.pl. Ponadto w przypadku awarii systemów informatycznych wykorzystywanych przez UODO dostęp do Państwa danych mogą mieć podmioty świadczące dla UODO pomoc serwisową.

Okres przechowywania danych.
Będziemy przechowywać Państwa dane osobowe do chwili zawiadomienia nas o odwołaniu inspektora ochrony danych bez jednoczesnego powiadomienia o wyznaczeniu nowej osoby, a następnie - zgodnie z obowiązującą w Urzędzie Ochrony Danych Osobowych Instrukcją kancelaryjną oraz przepisami o archiwizacji dokumentów - przez okres 5 lat od końca roku, w którym wpłynęło zawiadomienie o odwołaniu inspektora ochrony danych.

Prawa osób, których dane dotyczą.
Zgodnie z RODO przysługuje Państwu:
a) prawo dostępu do swoich danych oraz otrzymania ich kopii;
b) prawo do sprostowania (poprawiania) swoich danych;
c) prawo do usunięcia danych osobowych, w sytuacji, gdy przetwarzanie danych nie następuje w celu wywiązania się z obowiązku wynikającego z przepisu prawa lub w ramach sprawowania władzy publicznej;
d) prawo do ograniczenia przetwarzania danych;
e) prawo do wniesienia skargi do Prezes UODO (na adres Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00 - 193 Warszawa)

Informacja o wymogu podania danych.
Podanie przez Państwa danych osobowych w niniejszym formularzu jest obowiązkiem wynikającym z art. 37 ust. 7 RODO oraz art. 10 ustawy o ochronie danych osobowych.

Zawiadomienie o odwołaniu dotychczasowego inspektora ochrony danych i wyznaczeniu nowego (przetwarzanie danych w związku z zapobieganiem i zwalczaniem przestępczości)

Część A: Oznaczenie administratora danych

Pełna nazwa administratora: Kliknij tutaj, aby wprowadzić tekst.

REGON (jeśli został nadany) (opcjonalnie): Kliknij tutaj, aby wprowadzić tekst.

Adres:

Państwo	Kliknij tutaj, aby wprowadzić tekst.	Miejscowość	Kliknij tutaj, aby wprowadzić tekst.
Województwo	Kliknij tutaj, aby wprowadzić tekst.	Ulica	Kliknij tutaj, aby wprowadzić tekst.
Powiat	Kliknij tutaj, aby wprowadzić tekst.	Kod pocztowy	Kliknij tutaj, aby wprowadzić tekst.
Gmina	Kliknij tutaj, aby wprowadzić tekst.	Numer domu	Podaj numer
		Numer lokalu	Podaj numer

Osoba/osoby uprawnione do reprezentowania administratora

1.	Imię i nazwisko: Kliknij tutaj, aby wprowadzić tekst.	Stanowisko: Kliknij tutaj, aby wprowadzić tekst.
2.	Imię i nazwisko: Kliknij tutaj, aby wprowadzić tekst. (opcjonalnie)	Stanowisko: Kliknij tutaj, aby wprowadzić tekst. (opcjonalnie)
3.	Imię i nazwisko: Kliknij tutaj, aby wprowadzić tekst. (opcjonalnie)	Stanowisko: Kliknij tutaj, aby wprowadzić tekst. (opcjonalnie)
4.	Imię i nazwisko: Kliknij tutaj, aby wprowadzić tekst. (opcjonalnie)	Stanowisko: Kliknij tutaj, aby wprowadzić tekst. (opcjonalnie)
5.	Imię i nazwisko: Kliknij tutaj, aby wprowadzić tekst. (opcjonalnie)	Stanowisko: Kliknij tutaj, aby wprowadzić tekst. (opcjonalnie)

Część B: Dane dotychczasowego inspektora ochrony danych

Imię i nazwisko: Kliknij tutaj, aby wprowadzić tekst.

Część C: Dane kontaktowe inspektora ochrony danych

Imię: Kliknij tutaj, aby wprowadzić tekst. Nazwisko: Kliknij tutaj, aby wprowadzić tekst.

Telefon: Kliknij tutaj, aby wprowadzić tekst. Adres e-mail: Kliknij tutaj, aby wprowadzić tekst.

Powyżej musi zostać podany telefon lub adres e-mail (oba pola nie mogą pozostać puste – zgodnie z brzmieniem art. 10 ust. 1 ustawy o ochronie danych osobowych)

☐ Wniosek wypełniany przez pełnomocnika (opcjonalnie)

Pełnomocnictwo udzielone w formie elektronicznej oraz dowód uiszczenia opłaty skarbowej należy załączyć podczas składania wniosku przez portal biznes.gov.pl.
Pełnomocnictwo opatrzone kwalifikowanym podpisem elektronicznym osoby udzielającej pełnomocnictwa.

Administrator danych osobowych.
Administratorem Państwa danych osobowych będzie Prezes Urzędu Ochrony Danych Osobowych (Prezes UODO) z siedzibą w Warszawie, przy ul. Stawki 2.

Można się z nami kontaktować w następujący sposób:
a) listownie: ul. Stawki 2, 00-193 Warszawa
b) przez elektroniczną skrzynkę podawczą dostępną na stronie: https://www.uodo.gov.pl/pl/p/kontakt
c) telefonicznie: (22) 531 03 00

Inspektor ochrony danych.
Możecie się Państwo kontaktować również z wyznaczonym przez Prezesa UODO inspektorem ochrony danych:

- pod adresem email: iod@uodo.gov.pl
- listownie: Inspektor ochrony danych, Urząd Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa
- przez elektroniczną skrzynkę podawczą dostępną na stronie: https://uodo.gov.pl/pl/p/kontakt

Cele i podstawy przetwarzania.
Będziemy przetwarzać Państwa dane osobowe zawarte w formularzu w celu przyjmowania zawiadomień o danych kontaktowych inspektora ochrony danych zgodnie z art. 46 ust. 9 i 10 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, a następnie dla wypełnienia obowiązku archiwizacji dokumentów wynikającego z ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach.

Odbiorcy danych osobowych.
Odbiorcami Państwa danych osobowych mogą być Minister Cyfryzacji - jeśli zawiadomienie do Prezesa UODO zostało wysłane przez platformę ePUAP lub Minister Rozwoju i Technologii - jeśli korespondencja do Prezesa UODO przesłana została drogą elektroniczną za pośrednictwem formularzy zamieszczonych na platformie biznes.gov.pl. Ponadto odbiorcami Państwa danych mogą być podmioty, z którymi UODO zawarł umowę na świadczenie usług serwisowych dla użytkowanych w Urzędzie systemów informatycznych.

Okres przechowywania danych.
Będziemy przechowywać Państwa dane osobowe do chwili zawiadomienia nas o odwołaniu inspektora ochrony danych bez jednoczesnego powiadomienia o wyznaczeniu nowej osoby, a następnie - zgodnie z obowiązującą w Urzędzie Ochrony Danych Osobowych instrukcją kancelaryjną oraz przepisami o archiwizacji dokumentów wynikającymi z ustawy o narodowym zasobie archiwalnym i archiwach – przez okres 10 lat liczony od 1 stycznia roku następnego od daty wpływu ww. zawiadomienia o odwołaniu inspektora. Po upływie obowiązującego okresu przechowywania dokumentacja taka podlega ekspertyzie archiwalnej przeprowadzanej przez właściwe miejscowo archiwum państwowe, na podstawie której okres ten może zostać wydłużony.

Nieprawidłowe powiadomienia o wyznaczeniu inspektora ochrony danych oraz o zmianach w tym zakresie, w tym odwołaniu inspektora, przechowywane są przez okres 2 lat liczony od 1 stycznia roku następnego od daty wpływu zawiadomienia.

Prawa osób, których dane dotyczą.
Zgodnie z rozporządzeniem 2016/679 (RODO) przysługuje Państwu:
a) prawo dostępu do swoich danych oraz otrzymania ich kopii;
b) prawo do sprostowania (poprawiania) swoich danych;
c) prawo do ograniczenia przetwarzania danych;
d) prawo do usunięcia danych osobowych, w sytuacji, gdy przetwarzanie danych nie następuje w celu wywiązania się z obowiązku wynikającego z przepisu prawa;
e) prawo do wniesienia skargi do Prezesa UODO.

Informacja o wymogu podania danych.
Podanie przez Państwa danych osobowych w niniejszym formularzu jest obowiązkiem wynikającym z art. 46 ust. 9 i 10 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.

Zgłoszenie naruszenia ochrony danych osobowych

1. Typ zgłoszenia

Wskaż czy zgłaszasz naruszenie ochrony danych osobowych mające charakter jednorazowego zdarzenia (np. zgubienie, kradzież nośnika danych, przypadkowe wysłanie danych osobie nieuprawnionej), czy przygotowujesz wstępne zgłoszenie, które uzupełnisz później, lub czy uzupełniasz lub zmieniasz wcześniejsze zgłoszenie.

Podaj swoją sygnaturę sprawy (opcjonalnie)
(np. sygnatura w Twoim wewnętrznym rejestrze naruszeń) Kliknij tutaj, aby wprowadzić tekst.

◉ Zgłoszenie kompletne/jednorazowe	○ Zgłoszenie wstępne	○ Zgłoszenie uzupełniające/zmieniające
	Podaj przybliżoną datę uzupełnienia zgłoszenia (opcjonalnie) Kliknij tutaj, aby wprowadzić datę.	Podaj datę poprzedniego zgłoszenia (opcjonalnie) Kliknij tutaj, aby wprowadzić datę. Podaj sygnaturę sprawy UODO Kliknij tutaj, aby wprowadzić tekst.

☐ Naruszenie zostało lub zostanie zgłoszone organowi ochrony danych osobowych w innym państwie Jeśli tak, podaj w jakim.

☐ Naruszenie zostało lub zostanie zgłoszone innym organom np. Policja, CSIRT NASK, CSIRT GOV, CSIRT MON (najedź myszką na nazwę organu by dowiedzieć się więcej)

Podaj nazwy tych organów
Kliknij tutaj, aby wprowadzić tekst.

Podaj numer/sygnaturę zgłoszenia do innego organu
Kliknij tutaj, aby wprowadzić tekst.

2. Podmiot zgłaszający

2A. Dane administratora danych

Pełna nazwa administratora Kliknij tutaj, aby wprowadzić tekst.

REGON (opcjonalnie) Podaj numer. NIP (opcjonalnie) Podaj numer. KRS (opcjonalnie) Podaj numer.

Sektor (opcjonalnie) Dla sektora publicznego: Wybierz element. Dla sektora prywatnego: Wybierz element.

2B. Adres siedziby administratora danych

Ulica	Kliknij tutaj, aby wprowadzić tekst.	Numer domu	Podaj numer Numer lokalu Podaj numer
Miejscowość	Kliknij tutaj, aby wprowadzić tekst.	Kod pocztowy	Kliknij tutaj, aby wprowadzić tekst.
Gmina	Kliknij tutaj, aby wprowadzić tekst.	Powiat	Kliknij tutaj, aby wprowadzić tekst.
Województwo	Kliknij tutaj, aby wprowadzić tekst.	Państwo	Kliknij tutaj, aby wprowadzić tekst.

2C. Osoby uprawnione do reprezentowania administratora

1.	Imię i nazwisko	Kliknij tutaj, aby wprowadzić tekst.	Stanowisko	Kliknij tutaj, aby wprowadzić tekst.
2.	Imię i nazwisko	Kliknij tutaj, aby wprowadzić tekst.	Stanowisko	Kliknij tutaj, aby wprowadzić tekst.
3.	Imię i nazwisko	Kliknij tutaj, aby wprowadzić tekst.	Stanowisko	Kliknij tutaj, aby wprowadzić tekst.
4.	Imię i nazwisko	Kliknij tutaj, aby wprowadzić tekst.	Stanowisko	Kliknij tutaj, aby wprowadzić tekst.
5.	Imię i nazwisko	Kliknij tutaj, aby wprowadzić tekst.	Stanowisko	Kliknij tutaj, aby wprowadzić tekst.

2D. Pełnomocnik

☐ Wniosek wypełniany przez pełnomocnika (opcjonalnie)

Jeśli zgłoszenie przesyłane jest w formie elektronicznej, należy załączyć pełnomocnictwo **udzielone w formie elektronicznej** oraz dowód uiszczenia opłaty skarbowej

2E. Inspektor ochrony danych

Imię i nazwisko imię i nazwisko. Numer telefonu Numer telefonu. Adres e-mail E-mail.

☐ Inspektor nie został wyznaczony

Jeśli inspektor nie został wyznaczony podaj dane innego punktu kontaktowego, od którego można uzyskać więcej informacji o naruszeniu.

Kliknij tutaj, aby wprowadzić tekst.

2F. Inne podmioty uczestniczące w przetwarzaniu danych, których dotyczy naruszenie (opcjonalnie)

Podaj nazwy podmiotów, dane kontaktowe i wyjaśnij ich rolę w procesie przetwarzania, którego dotyczy naruszenie (np. podmiot przetwarzający, współadministratora, operator pocztowy itp.)

1.	Nazwa i dane kontaktowe	Kliknij tutaj, aby wprowadzić tekst.	Rola	Kliknij tutaj, aby wprowadzić tekst.
2.	Nazwa i dane kontaktowe	Kliknij tutaj, aby wprowadzić tekst.	Rola	Kliknij tutaj, aby wprowadzić tekst.
3.	Nazwa i dane kontaktowe	Kliknij tutaj, aby wprowadzić tekst.	Rola	Kliknij tutaj, aby wprowadzić tekst.
4.	Nazwa i dane kontaktowe	Kliknij tutaj, aby wprowadzić tekst.	Rola	Kliknij tutaj, aby wprowadzić tekst.
5.	Nazwa i dane kontaktowe	Kliknij tutaj, aby wprowadzić tekst.	Rola	Kliknij tutaj, aby wprowadzić tekst.

3. Czas naruszenia

3A. Wykrycie naruszenia i powiadomienie organu nadzorczego

Data stwierdzenia naruszenia
Wskaż kiedy dowiedziałeś/aś się o naruszeniu.
Jeśli nie znasz dokładnego terminu, podaj czas przybliżony.

Kliknij tutaj, aby wprowadzić datę.

Sposób stwierdzenia naruszenia
Np. zgłoszenie osoby której dane dotyczą czy cykliczny przegląd logów systemowych zgodnie z wdrożoną polityką bezpieczeństwa

Kliknij tutaj, aby wprowadzić tekst.

Data powiadomienia przez podmiot przetwarzający
(opcjonalnie)
Jeśli nie znasz dokładnego terminu, podaj czas przybliżony.

Kliknij tutaj, aby wprowadzić tekst.

Powody opóźnienia powiadomienia organu nadzorczego o naruszeniu
Pole obowiązkowe jeśli czas od momentu stwierdzenia naruszenia do czasu wypełniania formularza jest dłuższy niż 72h

Kliknij tutaj, aby wprowadzić tekst.

3B. Czas naruszenia

Data i czas zaistnienia/rozpoczęcia naruszenia
Jeśli nie znasz dokładnego terminu, podaj czas przybliżony.

Kliknij tutaj, aby wprowadzić tekst.

Data i czas zakończenia naruszenia
(opcjonalnie)
Jeśli nie znasz dokładnego terminu, podaj czas przybliżony.

Kliknij tutaj, aby wprowadzić tekst.

4. Charakter naruszenia

4A. Opisz szczegółowo na czym polegało naruszenie

Kliknij tutaj, aby wprowadzić tekst.

4B. Na czym polegało naruszenie?

☐ a) Zgubienie lub kradzież nośnika/urządzenia

☐ b) Dokumentacja papierowa (zawierająca dane osobowe) zgubiona, skradziona lub pozostawiona w niezabezpieczonej lokalizacji

☐ c) Korespondencja papierowa utracona przez operatora pocztowego lub otwarta przed zwróceniem jej do nadawcy

☐ d) Nieuprawnione uzyskanie dostępu do informacji

☐ e) Nieuprawnione uzyskanie dostępu do informacji poprzez złamanie zabezpieczeń

☐ f) Złośliwe oprogramowanie ingerujące w poufność, integralność lub dostępność danych

☐ g) Uzyskanie poufnych informacji przez pozornie zaufaną osobę w oficjalnej komunikacji elektronicznej, takiej jak e-mail czy komunikator internetowy (phishing)

☐ h) Nieprawidłowa anonimizacja danych osobowych w dokumencie

☐ i) Nieprawidłowe usunięcie/zniszczenie danych osobowych z nośnika/urządzenia elektronicznego przed jego zbyciem przez administratora

☐ j) Niezamierzona publikacja

☐ k) Dane osobowe wysłane do niewłaściwego odbiorcy

☐ l) Ujawnienie danych niewłaściwej osoby

☐ m) Ustne ujawnienie danych osobowych

4C. Działanie złośliwego oprogramowania (odpowiedz na poniższe pytania, jeśli w sekcji 4B zaznaczono pole f)

a) Jeśli w ocenie administratora doszło wyłącznie do naruszenia dostępności danych, w jaki sposób stwierdzono, że nie doszło do naruszenia ich poufności?
(w sytuacji gdy np. dane nie zostały pobrane przez osobę nieupoważnioną, a jedynie zaszyfrowane w sposób uniemożliwiający uzyskanie do nich dostępu)

Kliknij tutaj, aby wprowadzić tekst.

b) Czy, a jeżeli tak, to w jakiej formie, złośliwe oprogramowanie poinformowało o konieczności uiszczenia opłaty w celu odzyskania dostępu do danych (podaj nazwę złośliwego oprogramowania, sposób poinformowania, żądaną kwotę, kanał komunikacji, sposób zapłaty oraz termin)

Kliknij tutaj, aby wprowadzić tekst.

c) Jeżeli doszło do utraty dostępności danych, to czy administrator był w posiadaniu kopii zapasowej, jeśli tak to w jakim czasie ją przywrócił?

Kliknij tutaj, aby wprowadzić tekst.

UWAGA: *Jeżeli zgłoszenie naruszenia dotyczy podejrzanych załączników, phishingu, szantażu czy działania złośliwego oprogramowania, rozważ zgłoszenie zdarzenia do CERT Polska pod adresem https://incydent.cert.pl/. Dokonanie takiego zgłoszenia jest szczególnie zalecane w przypadku, kiedy odpowiedzi na powyższe pytania są utrudnione bądź niemożliwe.*
O fakcie zgłoszenia incydentu do CERT Polska poinformuj w zgłoszeniu uzupełniającym Prezesa UODO (pkt 1 formularza) podając datę zgłoszenia, jego numer oraz ewentualnie informacje na temat incydentu otrzymane od CERT Polska).

4D. Przyczyna naruszenia

- ☐ Wewnętrzne działanie niezamierzone
- ☐ Wewnętrzne działanie zamierzone
- ☐ Zewnętrzne działanie niezamierzone
- ☐ Zewnętrzne działanie zamierzone

4E. Charakter

- ☐ Naruszenie poufności danych
  Nieuprawnione lub przypadkowe ujawnienie bądź udostępnienie danych
- ☐ Naruszenie integralności danych
  Wprowadzenie nieuprawnionych zmian podczas odczytu, zapisu, transmisji lub przechowywania
- ☐ Naruszenie dostępności danych
  Brak możliwości wykorzystania danych na żądanie, w założonym czasie, przez osobę do tego uprawnioną

4F. Dzieci

☐ Naruszenie dotyczy przetwarzania danych w związku ze świadczeniem usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku.
(opcjonalnie)

5. Liczba osób i wpisów

Przybliżona liczba osób, których dotyczy naruszenie

Kliknij tutaj, aby wprowadzić tekst.

Przybliżona liczba wpisów danych osobowych, których dotyczy naruszenie
Nie dotyczy to liczby osób. Jednej osobie można przypisać kilka wpisów (np. jednej osobie można przypisać kilka wykonanych transakcji)

Kliknij tutaj, aby wprowadzić tekst.

6. Kategorie danych osobowych

UWAGA: W zgłoszeniu nie podawaj danych konkretnych osób, których dotyczy naruszenie.

6A. Dane podstawowe

- ☐ Nazwiska i imiona
- ☐ Imiona rodziców
- ☐ Data urodzenia
- ☐ Numer rachunku bankowego
- ☐ Adres zamieszkania lub pobytu
- ☐ Numer ewidencyjny PESEL
- ☐ Adres e-mail
- ☐ Nazwa użytkownika i/lub hasło
- ☐ Dane dotyczące zarobków i/lub posiadanego majątku
- ☐ Nazwisko rodowe matki
- ☐ Seria i numer dowodu osobistego
- ☐ Numer telefonu
- ☐ Wizerunek
- ☐ Inne, wskaż jakie:

Kliknij tutaj, aby wprowadzić tekst.

6B. Dane szczególnej kategorii

- ☐ Dane o pochodzeniu rasowym lub etnicznym
- ☐ Dane o poglądach politycznych
- ☐ Dane o przekonaniach religijnych lub światopoglądowych
- ☐ Dane o przynależności do związków zawodowych
- ☐ Dane dotyczące seksualności lub orientacji seksualnej
- ☐ Dane dotyczące zdrowia
- ☐ Dane genetyczne
- ☐ Dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej

6C. Dane, o których mowa w art. 10 RODO

☐ Dane dotyczące wyroków skazujących ☐ Dane dotyczące czynów zabronionych ☐ Inne

Kliknij tutaj, aby wprowadzić tekst.

7. Kategorie osób

☐ Pracownicy
☐ Użytkownicy
☐ Subskrybenci
☐ Studenci
☐ Uczniowie
☐ Służby mundurowe (np. wojsko, policja)
☐ Klienci (obecni i potencjalni)
☐ Klienci podmiotów publicznych
☐ Pacjenci
☐ Dzieci
☐ Osoby o szczególnych potrzebach (np. osoby starsze, niepełnosprawne itp.)

Szczegółowy opis kategorii osób, których dotyczy naruszenie:
Opisz np. kogo i w jakim przedziale czasowym dotyczy naruszenie
W zgłoszeniu nie podawaj danych konkretnych osób, których dotyczy naruszenie.

Kliknij tutaj, aby wprowadzić tekst.

8. Możliwe konsekwencje

8A. Uszczerbek fizyczny, majątkowy, niemajątkowy lub inne znaczące konsekwencje dla osoby, której dane dotyczą

☐ Utrata kontroli nad własnymi danymi osobowymi
☐ Ograniczenie możliwości realizowania praw z art. 15-22 RODO
☐ Ograniczenie możliwości realizowania praw
☐ Dyskryminacja
☐ Kradzież lub sfałszowanie tożsamości
☐ Strata finansowa
☐ Naruszenie dobrego imienia
☐ Utrata poufności danych osobowych chronionych tajemnicą zawodową
☐ Nieuprawnione odwrócenie pseudonimizacji
☐ Inne

Opisz poniżej inne skutki naruszenia prawa do ochrony danych osoby, której dane dotyczą:

Kliknij tutaj, aby wprowadzić tekst.

8B. Czy wystąpiło wysokie ryzyko naruszenia praw lub wolności osób fizycznych?

◉ Tak ○ Nie

Uzasadnienie

Kliknij tutaj, aby wprowadzić tekst.

9. Środki bezpieczeństwa i środki zaradcze

9A. Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa dotychczas stosowanych

Kliknij tutaj, aby wprowadzić tekst.

9B. Środki bezpieczeństwa zastosowane lub proponowane w celu zminimalizowana ryzyka ponownego wystąpienia naruszenia

Kliknij tutaj, aby wprowadzić tekst.

9C. Środki zastosowane lub proponowane w celu zaradzenia naruszeniu i zminimalizowania negatywnych skutków dla osób, których dane dotyczą

Kliknij tutaj, aby wprowadzić tekst.

10. Czy osoby, których dane dotyczą, zostały zawiadomione o naruszeniu?

◉ Tak	○ Nie, ale zostaną zawiadomione Pamiętaj, że po powiadomieniu osób, należy przesłać treść zawiadomienia do UODO.	○ Nie, nie zostaną zawiadomione, ponieważ:	○ Nie oceniłem jeszcze

Czy indywidualnie?

- (●) Tak
- ( ) Nie, gdyż indywidualne zawiadomienie każdej osoby, której dane dotyczą wymagałoby niewspółmiernie dużego wysiłku. W związku z tym został bądź zostanie wydany publiczny komunikat lub zastosowany podobny środek, za pomocą którego osoby, których dane dotyczą, zostały bądź zostaną poinformowane w równie skuteczny sposób.

Wskaż datę zawiadomienia
Kliknij tutaj, aby wprowadzić datę.

Wskaż datę planowanego zawiadomienia
Kliknij tutaj, aby wprowadzić datę.

Liczba zawiadomionych osób
Kliknij tutaj, aby wprowadzić tekst.

☐ Nie znam jeszcze daty kiedy zamierzam zawiadomić osoby, których dane dotyczą

Środki komunikacji wykorzystane do zawiadomienia osoby, której dane dotyczą
Kliknij tutaj, aby wprowadzić tekst.

Umieść zanonimizowaną treść zawiadomienia, którą przesłałeś bądź zamierzasz przesłać do osób, których dane dotyczą.
Pamiętaj, że zawiadomienie powinno:

- opisywać jasnym i prostym językiem charakter naruszenia ochrony danych osobowych,
- zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji,
- opisywać możliwe konsekwencje naruszenia ochrony danych osobowych,
- opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

Kliknij tutaj, aby wprowadzić tekst.

- ( ) przed naruszeniem wdrożono odpowiednie techniczne i organizacyjne środki ochrony (wskazane w pkt. 9A formularza) i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, anonimizacja czy pseudonimizacja uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych.
- ( ) po naruszeniu zastosowano środki (wskazane w pkt. 9C formularza) eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą.
- ( ) stwierdzono brak wysokiego ryzyka naruszenia praw lub wolności osób fizycznych (uzasadnienie w pkt. 8B formularza).

Jeśli jeszcze nie oceniłeś, czy zamierzasz zawiadomić osoby, których dane dotyczą, pamiętaj, że po podjęciu takiej decyzji będziesz musiał złożyć zgłoszenie uzupełniające.

11. Przetwarzanie transgraniczne

☐ Naruszenie ma charakter transgraniczny

Zaznacz kraje Europejskiego Obszaru Gospodarczego, których dotyczy naruszenie:

☐ Austria	☐ Belgia	☐ Bułgaria	☐ Chorwacja
☐ Cypr	☐ Czechy	☐ Dania	☐ Estonia
☐ Finlandia	☐ Francja	☐ Grecja	☐ Hiszpania
☐ Holandia	☐ Irlandia	☐ Islandia	☐ Liechtenstein
☐ Litwa	☐ Luksemburg	☐ Łotwa	☐ Malta
☐ Niemcy	☐ Norwegia	☐ Portugalia	☐ Rumunia
☐ Słowacja	☐ Słowenia	☐ Szwecja	☐ Węgry
☐ Wielka Brytania	☐ Włochy		

_____
Data, miejscowość
(dla zgłoszenia w formie papierowej)

_____
Podpis osoby lub osób upoważnionych do reprezentowania administratora[1]
(dla zgłoszenia w formie papierowej)

[1] Jeżeli zgłoszenie podpisuje pełnomocnik, należy pamiętać o załączeniu pełnomocnictwa

Informacja:

Administrator danych osobowych.
Administratorem Państwa danych osobowych będzie Prezes Urzędu Ochrony Danych Osobowych (Prezes UODO) z siedzibą w Warszawie, przy ul. Stawki 2.

Można się z nami kontaktować w następujący sposób:
a) listownie: ul. Stawki 2, 00-193 Warszawa
b) przez elektroniczną skrzynkę podawczą dostępną na stronie https://www.uodo.gov.pl/pl/p/kontakt
c) telefonicznie: (22) 531 03 00

Inspektor ochrony danych.
Możecie się Państwo kontaktować również z wyznaczonym przez Prezesa UODO inspektorem ochrony danych pod adresem email IOD@uodo.gov.pl

Cele i podstawy przetwarzania.
Będziemy przetwarzać Państwa dane osobowe zawarte w formularzu w celu przyjmowania zgłoszeń o naruszeniu ochrony danych osobowych zgodnie z art. 33 ust 1 , 3 i 4 RODO[1] bądź art. 44 ust. 1 – 5 DODO[2], podejmowania działań określonych w art. 34 ust. 4 oraz art. 58 ust. 2 RODO bądź art. 45 ust. 5 DODO, a także prowadzenia przez organ wewnętrznego rejestru naruszeń na podstawie art. 57 ust. 1 lit. u RODO. Następnie Państwa dane będziemy przetwarzać w celu wypełnienia obowiązku archiwizacji dokumentów wynikającego z ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach.

Odbiorcy danych osobowych.
Odbiorcami Państwa danych osobowych będą Minister Cyfryzacji w związku z zamieszczeniem formularza na platformie E-PUAP bądź Minister Przedsiębiorczości i Technologii w związku z zamieszczeniem formularza na platformie biznes.gov.pl

Okres przechowywania danych.
Będziemy przechowywać Państwa dane przez czas realizacji uprawnień Prezesa UODO wskazanych w art. 34 ust. 4 RODO i art. 58 ust. 2 RODO bądź art. 45 ust. 5 DODO, a następnie - zgodnie z obowiązującą w Urzędzie Prezesa UODO Instrukcją kancelaryjną oraz przepisami o archiwizacji dokumentów - przez okres 10 lat od końca roku, w którym zgłoszono naruszenie ochrony danych, lub - w przypadku skierowania wystąpienia lub wydania decyzji administracyjnej – wieczyście.

Prawa osób, których dane dotyczą.
Zgodnie z RODO przysługuje Państwu:
a) prawo dostępu do swoich danych oraz otrzymania ich kopii;
b) prawo do sprostowania (poprawiania) swoich danych;
c) prawo do usunięcia danych osobowych, w sytuacji, gdy przetwarzanie danych nie następuje w celu wywiązania się z obowiązku wynikającego z przepisu prawa lub w ramach sprawowania władzy publicznej;
d) prawo do ograniczenia przetwarzania danych;
e) prawo do wniesienia skargi do Prezesa UODO (na adres Prezesa Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00 - 193 Warszawa)

Informacja o wymogu podania danych.
Podanie przez Państwa danych osobowych w niniejszym formularzu jest obowiązkiem wynikającym z art. 33 ust. 3 RODO oraz z art. 63 § 2-3a ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego.

---

[1] 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 (RODO) oraz podjętych działań.

[2] Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości

Oświadczenie w sprawie wyrażenia zgody na przetwarzanie danych osobowych

Ja niżej popisana/podpisany na podstawie art. 6 ust. 1 lit. a, art. 9 ust. 2 lit. a 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) Dz.Urz. UE L 119/1 z 4.05.2016 (dalej „RODO") wyrażam zgodę na przetwarzanie następujących danych osobowych (imię, nazwisko, telefon, mail, adres, miejsce pracy, zajmowane stanowisko, pełnione funkcje, wybitne osiągnięcia naukowe, dziedzina i dyscyplina naukowa, tytuł lub stopień naukowy, tytuł zawodowy), w zakresie ……..…… .

Podanie przeze mnie danych osobowych jest dobrowolne.
Podane przeze mnie dane osobowe będą przetwarzane wyłącznie w celu ……..……..…… .

Jest mi wiadomym, że posiadam prawo do:

1) żądania od wskazanego w niniejszym oświadczeniu administratora danych osobowych:
   a) dostępu do moich danych osobowych,
   b) sprostowania moich danych osobowych,
   c) usunięcia moich danych osobowych, jeżeli zachodzi jedna z okoliczności wskazanych w art. 17 ust. 1 RODO i jeżeli przetwarzanie moich danych osobowych nie jest niezbędne w zakresie wskazanym w art. 17 ust. 3 RODO,
   d) ograniczenia przetwarzania moich danych osobowych w przypadkach wskazanych w art. 18 ust. 1 RODO,
2) wniesienia do wskazanego w niniejszym oświadczeniu administratora danych osobowych sprzeciwu wobec przetwarzania moich danych osobowych:
   a) na potrzeby marketingu bezpośredniego, w tym profilowania, w zakresie, w jakim przetwarzanie jest związane z takim marketingiem bezpośrednim,
   b) do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1 RODO, z przyczyn związanych z moją szczególną sytuacją, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym,
3) przenoszenia moich danych osobowych,
4) wniesienia skargi do organu nadzorczego, tj. do Prezesa Urzędu Ochrony Danych Osobowych, w przypadku uznania, że przetwarzanie moich danych osobowych narusza przepisy RODO,
5) wycofania w dowolnym momencie zgody na przetwarzanie moich danych osobowych.

Zapoznałam/em się z informacjami dotyczącymi przetwarzania moich danych osobowych zgodnie z art. 13 i 14 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), zamieszczonymi na stronie internetowej administratora danych.

……
data, miejsce i podpis osoby wyrażającej zgodę

Warszawa, dnia ……..

……
ul. ……..……
…-……. Warszawa
(Administrator danych osobowych)

Wnioskodawca:
……
ul. ……
…-……. Warszawa

WNIOSEK O USUNIĘCIE DANYCH OSOBOWYCH
(SKORZYSTANIE Z PRAWA DO BYCIA ZAPOMNIANYM)

Działając w imieniu własnym, na mocy o art. 17 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), Dz.Urz. UE L 119/1 z 4.05.2016 r. (dalej „RODO") wnoszę o usunięcie moich danych osobowych z bazy administratora danych osobowych oraz baz powiązanych, a także zaprzestania dalszego przetwarzania tych danych osobowych.

Żądanie zostało sformułowane w związku z faktem, iż przetwarzanie moich danych osobowych przestało być niezbędne do celów, dla których dane te zostały zebrane. W sytuacji braku spełnienia powyższego żądania, sprawa zostanie zgłoszona do Prezesa Urzędu Ochrony Danych Osobowych wraz z wnioskiem o ukaranie administratora danych osobowych na mocy z art. 83 RODO.

UZASADNIENIE

Zgodnie z art. 17 ust. 1 i 2 RODO osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi jedna z następujących okoliczności:

1. dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
2. osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie i nie ma innej podstawy prawnej przetwarzania;
3. osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania tych danych;
4. dane osobowe były przetwarzane niezgodnie z prawem;
5. dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie UE lub prawie państwa członkowskiego, któremu podlega administrator.

W przypadku, gdy została spełniona choć jedna przesłanka wymieniona w art. 17 ust. 1 RODO, administrator jest zobowiązany do usunięcia danych osobowych bez zbędnej zwłoki oraz poinformowania o tym fakcie osobę, którą usunięte dane dotyczą. Zobowiązanie administratora zostało rozszerzone także, o obowiązek poinformowania innych administratorów o żądaniu usunięcia danych.

……
data, miejsce i podpis wnioskodawcy

Umowa powierzenia przetwarzania danych osobowych

zawarta w dniu [data] w [miejscowość] pomiędzy**:**

[……] **– Administratorem**,
reprezentowanym przez: [……],
a
[……] – **Procesorem,**
reprezentowanym przez: [……],
(dalej jako „**Strony**").

PREAMBUŁA

Zważywszy, że:

a) Administrator oraz Podmiot przetwarzający są stronami umowy z dnia […] r. (dalej jako „**Umowa główna**"),
b) w związku z wykonywaniem Umowy głównej Procesor przetwarza dane powierzone mu przez Administratora dotyczące osób fizycznych,
c) Strony mają na celu zapewnienie zgodności przetwarzania danych osobowych zgodnie z obowiązującym prawem, jak również ochronę praw i wolność osób, których dane dotyczą,

zgodnie z art. 28 ust. 1-4 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. 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, dalej jako „RODO"), Strony postanowiły zawrzeć niniejszą umowę o powierzenie przetwarzania danych osobowych (dalej jako „**Umowa**").

§ 1 Przedmiot Umowy

1. Na podstawie Umowy Administrator powierza Procesorowi przetwarzanie danych osobowych wyłącznie w zakresie i w celu należytego wykonywania świadczeń określonych w Umowie głównej.
2. Powierzenie przetwarzania następuje w zakresie:
   Kategorie osób, których dane dotyczą: […].
   Rodzaj danych osobowych: […].
3. Procesor jest upoważniony do wykonywania następujących czynności przetwarzania powierzonych danych: 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.
4. Przetwarzanie przez Procesora powierzonych danych osobowych nastąpi przy wykorzystaniu systemów informatycznych Procesora.

§ 2 Oświadczenia i obowiązki Procesora

1. Procesor oświadcza, że posiada odpowiednie środki techniczne i organizacyjne, wiedzę, doświadczenie oraz wykwalifikowany personel w zakresie umożliwiającym należyte wykonanie Umowy, zgodnie z obowiązującymi przepisami prawa. Procesor oświadcza, że znane mu są zasady przetwarzania danych osobowych zawarte w RODO.
2. Procesor zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z Umową, RODO oraz innymi przepisami prawa powszechnie obowiązującego z zakresu ochrony danych osobowych.
3. Procesor jest odpowiedzialny za wszelkie naruszenia RODO lub Umowy spowodowane przez siebie lub podmioty z których usług korzysta, w tym w szczególności za udostępnienie lub wykorzystanie danych osobowych niezgodnie z Umową lub udostępnienie powierzonych do przetwarzania danych osobowych podmiotom lub osobom nieupoważnionym.
4. Procesor oświadcza i zobowiązuje się:
   a) przetwarzać dane osobowe wyłącznie na udokumentowane polecenie Administratora (jeśli nie wynika ono wprost z Umowy głównej) - co dotyczy też przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej - chyba że obowiązek taki nakłada na niego prawo Unii Europejskiej lub prawo polskie; w takim przypadku przed rozpoczęciem przetwarzania Procesor informuje Administratora o tym obowiązku prawnym,
   b) niezwłocznie poinformować Administratora, jeżeli jego zdaniem wydane mu polecenie stanowi naruszenie RODO lub innych obowiązujących przepisów z zakresu ochrony danych osobowych,
   c) stosować środki określone w art. 32 RODO, dotyczące bezpieczeństwa przetwarzania danych,
   d) udostępniać Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w RODO oraz umożliwić Administratorowi lub audytorowi upoważnionemu przez Administratora przeprowadzanie audytów i inspekcji,

e) korzystać z usług innego podmiotu przetwarzającego wyłącznie za uprzednią zgodą Administratora, wyrażoną w formie pisemnej pod rygorem nieważności,
f) pomagać Administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą,
g) pomagać Administratorowi wywiązać się z obowiązków określonych w art. 32-36 RODO,
h) udostępnić Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 RODO oraz umożliwić Administratorowi lub audytorowi upoważnionemu przez Administratora przeprowadzanie audytów i inspekcji.

5. Procesor dopuści do przetwarzania danych osobowych wyłącznie osoby, które:
   a) zostały upoważnione do przetwarzania danych osobowych, na podstawie pisemnego upoważnienia wydanego im przez Procesora,
   b) złożyły w formie pisemnej oświadczenie o zachowaniu w poufności powierzonych im danych.
6. Procesor zobowiązuje się do ograniczenia dostępu do danych wyłącznie do osób, których dostęp do danych jest potrzebny do realizacji Umowy.
7. Procesor zobowiązany jest przedstawić na każde żądanie Administratora dokumenty, o których mowa w ust. 5, jak również wszelkie inne, w tym także udzielić wszelkich niezbędnych informacji, dotyczących przetwarzania danych osobowych w zakresie określonym Umową.
8. Procesor niezwłocznie poinformuje Administratora, jeżeli jego zdaniem wydane mu polecenie stanowi naruszenie RODO lub innych obowiązujących przepisów z zakresu ochrony danych osobowych.
9. Jeżeli Procesor w celu realizacji Umowy lub Umowy Głównej wykorzystuje zautomatyzowane przetwarzanie, w tym profilowanie, o którym mowa w art. 22 ust. 1 i 4 RODO, Procesor informuje o tym Administratora w celu wykonania przez Administratora obowiązku informacyjnego.

§ 3 Dalsze powierzenie przetwarzania

1. W celu realizacji Umowy, Procesor nie może korzystać z usług innego podmiotu przetwarzającego bez uzyskania uprzedniej zgody Administratora, wyrażonej w formie pisemnej pod rygorem nieważności.
2. W przypadku ogólnej pisemnej zgody, Procesor informuje Administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, umożliwiając Administratorowi wyrażenie sprzeciwu wobec takich zmian w terminie 2 dni roboczych od dnia zawiadomienia o zamiarze dalszego powierzenia / podpowierzenia.
3. W razie korzystania z usług innego podmiotu przetwarzającego Procesor przestrzega warunków określonych w art. 28 ust. 4 RODO, tj. Procesor zapewnia w umowie z dalszym podmiotem przetwarzającym, że nałożone zostają na niego te same obowiązki ochrony danych osobowych jak w Umowie powierzenia, w szczególności obowiązek wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie danych odpowiadało wymogom RODO, jak również wszelkie inne obowiązki ochrony danych, jakimi na podstawie Umowy objęty jest Procesor. Administrator może w każdej chwili zażądać od Procesora przedstawienia umowy z dalszym podmiotem przetwarzającym lub jej wzoru jeszcze przed jej zawarciem.
4. Jeżeli dalszy podmiot przetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec Administratora za wypełnienie obowiązków tego innego podmiotu przetwarzającego spoczywa na Procesorze.
5. W przypadku dalszego powierzenia przetwarzania danych osobowych Procesor zobowiązuje się do zawarcia w umowach z dalszymi podmiotami przetwarzającymi postanowień, zgodnie z którymi umowy dalszego przetwarzania danych będą ulegały rozwiązaniu z chwilą rozwiązania Umowy.

§ 4 Audyt / Inspekcje

1. Administrator ma prawo kontroli realizacji przez Procesora obowiązków, o których mowa w Umowie. Kontrola może zostać przez Administratora przeprowadzona w każdym czasie i w każdej formie. Kontrola następuje w formie audytów, w tym inspekcji.
2. Administrator poinformuje Procesora co najmniej na 2 dni robocze przed planowaną datą audytu i/lub inspekcji o zamiarze jego/jej przeprowadzenia.
3. Audyt obejmuje zbadanie zgodności przetwarzania danych osobowych przez Procesora z Umową oraz obowiązującymi przepisami prawa, w szczególności Administrator może przeprowadzić weryfikację zgodności i adekwatności środków technicznych i organizacyjnych zabezpieczających przetwarzanie danych osobowych wdrożonych przez Procesora.
4. Inspekcja obejmuje prawo:
   a) wstępu do pomieszczeń, w których znajdują się zasoby uczestniczące w operacjach przetwarzania powierzonych danych osobowych,

b) żądania złożenia pisemnych lub ustnych wyjaśnień od osób upoważnionych do przetwarzania powierzonych danych osobowych,
c) wglądu do wszelkich dokumentów i wszelkich danych mających bezpośredni związek z celem inspekcji,
d) przeprowadzania oględzin urządzeń, nośników oraz systemów informatycznych służących do przetwarzania powierzonych danych.

5. Procesor ma obowiązek współpracować z Administratorem i upoważnionymi przez niego audytorami, w szczególności zapewniać im dostęp do pomieszczeń i dokumentów obejmujących dane osobowe oraz informacje o sposobie przetwarzania danych osobowych, infrastruktury teleinformatycznej oraz urządzeń IT, a także umożliwić kontakt z osobami mającymi wiedzę na temat procesów przetwarzania danych osobowych.
6. W przypadku stwierdzenia podczas audytu i/lub inspekcji uchybień, Procesor zobowiązuje się do ich usunięcia w terminie wskazanym przez Administratora danych.
7. Z przeprowadzonego audytu, inspekcji przedstawiciel Administratora danych sporządza protokół pokontrolny, który podpisują przedstawiciele obu Stron. Procesor zobowiązuje się w terminie uzgodnionym z Administratorem, dostosować do zaleceń pokontrolnych zawartych w protokole, w tym w szczególności usunąć wszelkie uchybienia w zakresie przetwarzania danych osobowych.
8. Procesor jest zobowiązany zapewnić w umowie z dalszym podmiotem przetwarzającym możliwość przeprowadzania przez Administratora audytu zgodności przetwarzania danych osobowych przez dalszy podmiot przetwarzający na zasadach określonych w Umowie.
9. Procesor nie ma prawa żądania od Administratora zapłaty jakiegokolwiek wynagrodzenia z tytułu przeprowadzonego audytu lub zwrotu kosztów lub podniesienia innych roszczeń z tym związanych.

§ 5 Raportowanie / Zawiadomienie o naruszeniu

1. Na żądanie Administratora, Procesor udostępnia wszelkie informacje niezbędne do realizacji lub wykazania spełnienia obowiązków wynikających z RODO. Informacji tych udziela się w terminie 5 dni od dnia doręczenia wniosku, z zastrzeżeniem ust. 3. Jeżeli żądanie dotyczy realizacji obowiązku zgłoszenia naruszenia ochrony danych osobowych lub usunięcia jego skutków, Procesor udziela informacji niezwłocznie, nie później niż w ciągu 24 godzin od doręczenia żądania, które może zostać doręczone za pośrednictwem poczty elektronicznej na adres e-mail: […]. Udzielenie informacji następuje za pośrednictwem poczty elektronicznej na adres e-mail: […]. Jednocześnie Procesor dokonuje zawiadomienia listownie na adres siedziby Administratora.
2. Jeżeli Procesor wykryje naruszenie ochrony danych osobowych, zgłasza je Administratorowi niezwłocznie, nie później niż w ciągu 24 godzin od wykrycia naruszenia lub od chwili powzięcia przez Procesora podejrzenia o takim naruszeniu (w zależności od tego, które z tych zdarzeń wystąpi jako pierwsze). Procesor zobowiązuje się do zawiadomienia Administratora zarówno o każdym przypadku naruszenia Umowy, RODO lub innych przepisów z zakresu prawa ochrony danych osobowych, jak i o każdym przypadku podejrzenia takiego naruszenia. Zawiadomienie następuje za pośrednictwem poczty elektronicznej na adres e-mail: […]. Jednocześnie Procesor dokonuje zawiadomienia listownie na adres siedziby Administratora.
3. Udzielnie informacji i/lub zawiadomienie, o których mowa w ust. 1 i 2, w zakresie naruszenia lub/i podejrzenia naruszenia opisuje szczegółowo wszystkie okoliczności faktyczne i prawne naruszenia lub podejrzenia naruszenia i podjęte przez Procesora środki zaradcze (naprawcze). Dla skuteczności zawiadomienia Procesor zobowiązany jest do uzyskania od Administratora potwierdzenia otrzymania wiadomości e-mail. Zawiadomienie nie wyłącza, ani nie ogranicza innych obowiązków Procesora wynikających z niniejszej Umowy, RODO lub innych przepisów prawa ochrony danych osobowych.
4. Niezależnie od wskazanego powyżej zawiadomienia, Procesor niezwłocznie informuje Administratora o:
   a) jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania powierzonych danych osobowych,
   b) wydaniu jakiegokolwiek orzeczenia dotyczącego przetwarzania powierzonych danych osobowych,
   c) wszelkich planowanych lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania powierzonych danych osobowych.
5. Niezależnie od obowiązków wskazanych powyżej, Procesor niezwłocznie podejmie wszelkie wymagane okolicznościami działania mające na celu ograniczenie i naprawienie negatywnych skutków naruszenia.
6. Procesor jest zobowiązany do dokumentowania wszelkich naruszeń ochrony powierzonych mu danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutków oraz podjętych działań naprawczych. Podmiot przetwarzający jest zobowiązany na każde żądanie Administratora niezwłocznie udostępnić mu dokumentację, o której mowa powyżej.
7. Procesor dostarczy Administratorowi na każde jego wezwanie, nie później niż w terminie 5 dni roboczych od momentu zgłoszenia żądania, wszelkie dowody na to, że zastosował środki techniczne i organizacyjne.

8. Procesor powinien także dostarczyć dowody na wdrożenie wspomnianych środków, mogące mieć formę:
   a) spełniania zatwierdzonych zasad postępowania zgodnie z art. 40 RODO,
   b) certyfikacji na podstawie zatwierdzonej procedury certyfikacyjnej zgodnie z art. 42 RODO,
   c) ostatnich wyników audytów, raportów lub wyciągów z raportów sporządzonych przez niezależne podmioty (biegli rewidenci, inspektorzy ochrony danych, biura bezpieczeństwa IT, audytorzy ochrony danych, audytorzy jakości),
   d) odpowiedniej certyfikacji udzielonej przez bezpieczeństwo IT lub audyt ochrony danych.

§ 6 Odpowiedzialność Podmiotu przetwarzającego

1. Procesor ponosi względem Administratora danych pełną odpowiedzialność za wykonanie, niewykonanie lub nienależyte wykonanie Umowy, w tym w szczególności za przetwarzanie powierzonych danych osobowych niezgodnie z Umową, RODO lub innymi obowiązującymi przepisami prawa z zakresu ochrony danych.
2. Procesor ponosi pełną odpowiedzialność za wszelkie szkody wyrządzone osobom trzecim, które powstały w związku z niewykonaniem lub nienależytym wykonaniem Umowy przez Procesora lub w związku z naruszeniem przepisów prawa obowiązującego ochrony danych osobowych, w szczególności RODO.
3. W przypadku wystąpienia przez osoby, których dane zostały powierzone do przetwarzania, z roszczeniami do Procesora, Procesor niezwłocznie poinformuje o tym fakcie Administratora.
4. Jeżeli wskutek naruszenia postanowień Umowy, RODO lub innych przepisów prawa z zakresu ochrony danych osobowych przez Procesora, Administrator będzie zobowiązany do zapłaty odszkodowania, administracyjnej kary pieniężnej lub zostanie w inny sposób pociągnięty do odpowiedzialności za naruszenie przepisów o ochronie danych osobowych, Procesor zobowiązuje się do naprawienia Administratorowi poniesionych szkód w pełnej wysokości, w szczególności zwracając Administratorowi kwoty wypłaconych odszkodowań lub uiszczonych administracyjnych kar pieniężnych, jak również wyrównując koszty wykonania jakichkolwiek innych nałożonych lub odnoszących się do Administratora obowiązków bądź sankcji. Na żądanie Administratora, Procesor zwolni Administratora z odpowiedzialności oraz zaspokoi roszczenia takich osób lub podmiotów je zgłaszających, lub wyłoży kwoty konieczne do pokrycia wszelkich roszczeń i kosztów, o których mowa powyżej (w tym także koszty pomocy prawnej).
5. Na zasadach, o których mowa powyżej, Procesor ponosi pełną odpowiedzialność za działania lub zaniechania dalszego podmiotu przetwarzającego.
6. Na zasadach, o których mowa powyżej, Procesor ponosi odpowiedzialność za działania lub zaniechania swoich pracowników zleceniobiorców lub i innych osób, przy pomocy których przetwarza powierzone dane osobowe, jak za własne działania lub zaniechania.

§ 7 Kary umowne

1. W razie naruszenia jakiegokolwiek postanowienia Umowy, w tym w szczególności przetwarzania powierzonych danych osobowych niezgodnie z Umową lub przepisami prawa, w szczególności w razie udostępnienia danych osobowych osobom nieupoważnionym, Procesor będzie zobowiązany do zapłaty na rzecz Administratora za każde naruszenie kary umownej w wysokości […].
2. W razie udostępnienia danych osobowych osobom nieupoważnionym lub przetwarzania powierzonych danych osobowych niezgodnie z warunkami niniejszej Umowy, Procesor będzie obowiązany do zapłaty na rzecz Administratora kary umownej w wysokości […].
3. W przypadku rozwiązania Umowy ze skutkiem natychmiastowym, Procesor będzie zobowiązany do zapłaty na rzecz Administratora kary umownej w wysokości […].
4. Administratorowi przysługuje prawo dochodzenia odszkodowania w wysokości przewyższającej zastrzeżoną karę umowną na zasadach ogólnych.
5. Kary umowne należne od Procesora kumulują się.
6. Dla uniknięcia wątpliwości Strony zgodnie postanawiają, że rozwiązanie przez Administratora Umowy ze skutkiem natychmiastowym nie powoduje utraty mocy postanowień o karze umownej lub odpowiedzialności odszkodowawczej Procesora.

§ 8 Czas trwania i rozwiązanie Umowy

1. Umowa zostaje zawarta nie dłużej niż na czas trwania Umowy głównej.
2. Każda ze stron może wypowiedzieć Umowę z zachowaniem [**….**] okresu wypowiedzenia.
3. Administrator uprawniony jest do rozwiązania Umowy ze skutkiem natychmiastowym w przypadku zaistnienia ważnych powodów, w tym w szczególności:
   a) spełniania zatwierdzonych zasad postępowania zgodnie z art. 40 RODO,
   b) w razie naruszenia przez Procesora lub dalszy podmiot przetwarzający postanowień Umowy lub przepisów RODO lub innych obowiązujących przepisów prawa, lub

c) organ nadzorczy stwierdzi, że Procesor lub dalszy podmiot przetwarzający nie przestrzega zasad przetwarzania danych osobowych, lub
d) Administrator, w wyniku przeprowadzenia audytu, stwierdzi, że Procesor lub dalszy podmiot przetwarzający nie przestrzega zasad przetwarzania danych osobowych wynikających z Umowy lub RODO lub innych obowiązujących przepisów prawa, lub
e) Procesor nie zastosuje się do zaleceń pokontrolnych w uzgodnionym terminie, lub
f) Procesor nie zgłosi Administratorowi naruszenia w określonym Umową terminie, lub
g) Procesor powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody Administratora.

§ 9 Odpowiadanie na żądania osoby, której dane dotyczą

1. Na wniosek Administratora, Procesor stosuje środki organizacyjne i techniczne, umożliwiające Administratorowi wywiązanie się z obowiązku odpowiadania na żądania osoby, której dane dotyczą.
2. W razie wpływu do Procesora żądania w zakresie realizacji praw osób, których dotyczą powierzone dane, Procesor niezwłocznie informuje o tym Administratora. Udzielając informacji, Procesor przekazuje dane nadawcy i treść żądania oraz określa, w jakim zakresie jest w stanie przyczynić się do realizacji żądania.

§ 10 Usunięcie lub zwrot danych osobowych

1. Po zakończeniu świadczenia usług z Umowy głównej, zależnie od decyzji Administratora Procesor usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii Europejskiej lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.
2. Procesor jest zobowiązany wykonać decyzję, o której mowa w ust. 1, w terminie 7 dni od dnia jej doręczenia. Procesor zobowiązany jest do przekazania Administratorowi protokołu usunięcia danych osobowych.

§ 11 Rejestr czynności przetwarzania danych osobowych

1. W zakresie objętym Umową, Procesor zobowiązuje się do prowadzenia w imieniu Administratora Rejestru czynności przetwarzania danych osobowych, zgodnie z art. 30 RODO.
2. Procesor udostępniania na żądanie Administratora prowadzony rejestr czynności przetwarzania danych.

§ 12 Miejsce przetwarzania danych osobowych

1. Miejsce przetwarzania danych osobowych
2. Procesor będzie przetwarzać dane osobowe jedynie na obszarze EOG. Procesor bez uzyskania uprzedniego polecenia Administratora, wyrażonego w formie pisemnej pod rygorem nieważności, nie może przekazywać danych osobowych do państw trzecich.

§ 13 Wynagrodzenie

1. Umowa jest nieodpłatna. Procesor nie jest uprawniony do żądania od Administratora jakiegokolwiek dodatkowego wynagrodzenia z tytułu realizacji Umowy, ani też zwrotu jakichkolwiek kosztów związanych z realizacją praw lub zobowiązań wynikających z Umowy.

§ 14 Postanowienia końcowe

1. Umowa podlega prawu polskiemu.
2. Procesor nie może przenieść praw lub obowiązków wynikających z Umowy bez uprzedniej zgody Administratora wyrażonej w formie pisemnej pod rygorem bezskuteczności.
3. Umowa uchyla i zastępuje wszelkie postanowienia dotyczące powierzenia przetwarzania danych osobowych zawarte w Umowie głównej.
4. Wszelkie zmiany Umowy wymagają porozumienia Stron w formie pisemnej pod rygorem nieważności.
5. W przypadku stwierdzenia, że którekolwiek z postanowień Umowy było w momencie jej zawarcia z mocy prawa nieważne lub bezskuteczne, okoliczność ta nie będzie miała wpływu na ważność, skuteczność lub możliwość wyegzekwowania pozostałych jej postanowień. W razie zajścia takiej sytuacji, Strony zobowiązują się zawrzeć aneks do Umowy, w którym sformułują postanowienia zastępcze, których cel będzie równoważny lub możliwie najbardziej zbliżony do celu postanowień nieważnych lub bezskutecznych. W przypadku nieosiągnięcia porozumienia zastosowanie będą miały odpowiednie przepisy prawa.
6. Wszelkie spory pomiędzy Stronami powstałe w związku z realizacją Umowy, będą rozstrzygane przez sąd właściwy ze względu na siedzibę [….].
7. W sprawach nieuregulowanych Umową znajdują zastosowanie przepisy obowiązującego prawa.
8. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.
9. Załącznikiem stanowiącym integralną część Umowy jest klauzula informacyjna (art. 14 ust. 1-2 RODO), Polityka ochrony danych osobowych Procesora oraz aktualne odpisy KRS Stron.

…….. ……..……
(podpis) (podpis)

Umowa udostępnienia danych osobowych

zawarta w ……..., w dniu …… roku, pomiędzy:

……, wpisanym do Rejestru Stowarzyszeń Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy ……..., ……. Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS: ……., NIP: ……., REGON: …….. (dalej jako „**A**"), reprezentowanym przez:
…… – ……,
oraz
…….. z siedzibą w ……., adres: ul. ……., ……., wpisaną do Rejestru Przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy ……..., ……. Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS: ……., posiadającą kapitał zakładowy w wysokości: …….. zł, NIP: ……..., REGON: ……... (dalej jako „**B**"), reprezentowaną przez:
…… – ……,
(dalej łącznie jako „**Strony**", a każda z nich z osobna jako „**Strona**").

§ 1 Definicje

1. Ilekroć niniejsza umowa stanowi o:
   1) **Danych Osobowych** – należy przez to rozumieć dane osobowe udostępnione A przez B w okresie obowiązywania niniejszej umowy,
   2) **RODO** – należy przez to rozumieć 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),
   3) **Umowie głównej** – należy przez to rozumieć umowę nr …….,
   4) **Umowie** – należy przez to rozumieć niniejszą umowę.
2. Pojęcia nie zdefiniowane w Umowie mają znaczenie nadane im w RODO.

§ 2 Przedmiot i cel Umowy

1. Dla celów związanych z zawarciem oraz realizacją Umowy głównej, B udostępni A dane osobowe:
   1) osób wchodzących w skład zespołu ds. realizacji projektu (dalej jako „**członkowie zespołu ds. realizacji projektu**"),
   2) pracowników przypisanych do projektu (dalej jako „**pracownicy**").
2. Udostępnienie danych osobowych **członków zespołu ds. realizacji projektu** nastąpi w zakresie danych, takich jak: imię, nazwisko, pełniona funkcja, a także numer PESEL.
3. Udostępnienie danych osobowych **pracowników** nastąpi w zakresie danych takich jak: imię, nazwisko, funkcja.
4. Udostępnienie danych przedstawicieli oraz osób wyznaczonych do kontaktu (dalej łącznie jako „**osoby do kontaktów**") nastąpiło w zakresie określonym Umową główną.
5. Za udostępnienie innych danych niż wskazane powyżej, B ponosi wyłączną odpowiedzialność.

§ 3 Oświadczenia i obowiązki B

1. B oświadcza, że udostępnione A dane osobowe zebrał zgodnie z RODO, posiada stosowną podstawę prawną do ich przetwarzania, w tym także udostępnienia ich A i ponosi z tego tytułu pełną odpowiedzialność względem A oraz osób, których dane dotyczą, jak również odpowiedzialność względem organu nadzorczego, w szczególności z tytułu administracyjnych kar pieniężnych.
2. B zobowiązuje się zapewnić, aby udostępnienie A danych osobowych było dopuszczalne i legalne na mocy przepisów RODO przez cały okres obowiązywania Umowy.
3. Z chwilą udostępnienia danych osobowych A, B zobowiązuje się spełnić obowiązek informacyjny w imieniu A względem członków zespołu ds. realizacji projektu, pracowników, osób do kontaktów, zgodnie z klauzulą informacyjną stanowiącą załącznik do Umowy. Spełnienie wskazanego obowiązku informacyjnego nastąpi zgodnie z treścią art. 14 RODO.

4. B zobowiązuje się pomagać A poprzez odpowiednie środki techniczne i organizacyjne, w wywiązywaniu się z obowiązku odpowiadania na żądania osób, których dane dotyczą, w zakresie wykonywania ich praw określonych w RODO. W tym celu B zobowiązuje się do udzielenia A wszelkiego wymaganego wsparcia, umożliwiającego realizację praw osoby, której dane dotyczą, w szczególności w zakresie prawa dostępu do swoich danych, prawa do sprostowania danych, prawa do bycia zapomnianym, prawa do ograniczenia przetwarzania oraz wszelkich innych określonych w RODO.
5. B niniejszym oświadcza, że wdrożył odpowiednie środki techniczne i organizacyjne w celu zapewnienia zgodności przetwarzania danych osobowych z RODO, oraz innymi przepisami prawa.
6. B oświadcza i zobowiązuje się ponadto:
   1) stosować środki określone w art. 32 RODO, dotyczące bezpieczeństwa przetwarzania danych osobowych przez cały okres obowiązywania Umowy,
   2) niezwłocznie informować A o każdym naruszeniu ochrony danych osobowych, które może mieć wpływ na interes prawny A,
   3) udostępniać A wszelkie informacje niezbędne do spełnienia obowiązków określonych w RODO, w tym w szczególności wymagane do zgłoszenia naruszenia ochrony danych osobowych zgodnie z art. 33 i 34 RODO,
   4) umożliwić A, w tym audytorowi upoważnionemu, przeprowadzenie audytów,
   5) korzystać z usług takiego podmiotu przetwarzającego w ramach realizacji Umowy, który zapewnia gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.
7. Każda ze Stron we własnym zakresie prowadzi rejestr czynności przetwarzania (art. 30 RODO).

§ 4 Odpowiedzialność B (RODO)

1. B podnosi względem A oraz osób, których dane dotyczą, jak również względem organu nadzorczego, pełną odpowiedzialność za legalność, poprawność, kompletność oraz aktualność danych osobowych.
2. B ponosi pełną odpowiedzialność za wszelkie naruszenia RODO lub Umowy spowodowane przez B lub podmioty z których usług korzysta, w tym w szczególności za zebranie i udostępnienie danych osobowych niezgodnie z RODO lub Umową.

§ 5 Audyt

1. A jest uprawniony do kontroli realizacji przez B obowiązków określonych Umową. Kontrola może zostać przez A przeprowadzona w każdym czasie. Kontrola następuje w formie audytów.
2. Audyt obejmuje zbadanie zgodności przetwarzania danych osobowych przez B z Umową, RODO lub innymi przepisami z zakresu ochrony danych osobowych.
3. A informuje B co najmniej na 5 dni roboczych przed datą audytu o zamiarze jego przeprowadzenia
4. B ma obowiązek współpracować z A i upoważnionymi przez niego audytorami, w szczególności zapewnić im dostęp do pomieszczeń i dokumentów obejmujących dane osobowe określone Umową oraz udzielić A informacji o sposobie przetwarzania danych osobowych oraz wszelkich innych, wymaganych przez A.

§ 6 Zawiadomienie o naruszeniu

1. Na każde żądanie A, B udostępnia wszelkie informacje niezbędne do realizacji lub wykazania spełnienia przez A obowiązków wynikających z RODO.
2. Informacji, o których mowa w ust. 1, B udziela A, niezwłocznie, nie później niż w ciągu 24 godzin od chwili zgłoszenia przez A żądania na adres e-mail: […].
3. B zobowiązuje się do zawiadomienia A, o każdym przypadku naruszenia RODO lub innych przepisów z zakresu prawa ochrony danych osobowych objętych Umową, jak i o każdym przypadku podejrzenia takiego naruszenia.
4. Zawiadomienie, o którym mowa w ust. 3, powinno nastąpić niezwłocznie, nie później jednak niż w terminie 24 godzin od chwili jego wykrycia przez B lub od chwili powzięcia przez B podejrzenia o takim naruszeniu na adres e-mail: […]. Jednocześnie B dokonuje zawiadomienia listownie na adres siedziby A, co w żadnym stopniu nie zwalania B z odpowiedzialności względem A lub osób, które dane dotyczą.

5. B niezwłocznie informuje A także o:
   1) każdym postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania danych osobowych objętych Umową,
   2) wydaniu jakiegokolwiek orzeczenia dot. przetwarzania danych osobowych objętych Umową,
   3) wszelkich planowanych lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania danych osobowych objętych Umową.
6. B jest zobowiązany do dokumentowania wszelkich naruszeń ochrony danych osobowych objętych Umową, w tym okoliczności naruszenia ochrony danych osobowych, jego skutków oraz podjętych działań zaradczych. B jest zobowiązany na każde żądanie A niezwłocznie udostępnić mu dokumentację, o której mowa powyżej. Dotyczy to także dokumentacji znajdującej się w posiadaniu podmiotu przetwarzającego B.

§ 7 Odpowiedzialność B

1. B ponosi względem A pełną odpowiedzialność za niewykonanie lub nienależyte wykonanie Umowy, w tym w szczególności za przetwarzanie danych osobowych niezgodnie z Umową, RODO lub innymi obowiązującymi przepisami prawa z zakresu ochrony danych osobowych.
2. B ponosi pełną odpowiedzialność za wszelkie szkody wyrządzone osobom, których dane dotyczą, które powstały w związku z niewykonaniem lub nienależytym wykonaniem Umowy przez B lub w związku z naruszeniem RODO lub innych przepisów prawa ochrony danych osobowych.
3. Jeżeli wskutek naruszenia przez B lub podmioty działające w imieniu lub na rzecz B, postanowień Umowy, RODO lub innych przepisów prawa z zakresu ochrony danych osobowych, A będzie zobowiązany do zapłaty odszkodowania, administracyjnej kary pieniężnej lub zostanie w inny sposób pociągnięty do odpowiedzialności za naruszenie przepisów o ochronie danych osobowych, B zobowiązuje się do naprawienia A poniesionych szkód w pełnej wysokości, w szczególności zwracając A kwoty wypłaconych odszkodowań lub uiszczonych administracyjnych kar pieniężnych, jak również wyrównując koszty wykonania jakichkolwiek innych nałożonych lub odnoszących się do A obowiązków bądź sankcji. B zwolni A z odpowiedzialności oraz zaspokoi roszczenia takich osób lub podmiotów je zgłaszających, lub wyłoży kwoty konieczne do pokrycia wszelkich roszczeń i kosztów, o których mowa powyżej, w tym także koszty pomocy prawnej.
4. Na zasadach, o których mowa powyżej, B ponosi pełną odpowiedzialność za działania lub zaniechania swoich pracowników, zleceniobiorców lub i innych osób, przy pomocy których przetwarza dane osobowe, jak za własne działania lub zaniechania.
5. Na zasadach, o których mowa powyżej, B ponosi pełną odpowiedzialność za działania lub zaniechania jego podmiotu przetwarzającego, jak za własne działania lub zaniechania.

§ 8 Kary umowne

1. W razie naruszenia przez B któregokolwiek z postanowień Umowy w zakresie przetwarzania danych osobowych, w tym w szczególności w razie udostępnienia danych osobowych bez podstawy prawnej lub niezgodnie z Umową, B będzie zobowiązany do zapłaty na rzecz A za każde naruszenie kary umownej w wysokości […].
2. W przypadku rozwiązania przez A Umowy ze skutkiem natychmiastowym, B będzie zobowiązany do zapłaty na rzecz A kary umownej w wysokości […].
3. We wszystkim przypadkach, w których została zastrzeżona dla A kara umowna, A przysługuje prawo dochodzenia od B odszkodowania na zasadach ogólnych.
4. Kary umowne należne kumulują się.
5. Dla uniknięcia wątpliwości Strony zgodnie postanawiają, że rozwiązanie przez A Umowy ze skutkiem natychmiastowym nie powoduje utraty mocy postanowień o karze umownej lub odpowiedzialności odszkodowawczej B.

§ 9 Czas trwania i rozwiązanie Umowy

1. Z zastrzeżeniem, o którym mowa w § 9 ust. 2, Umowa zostaje zawarta na czas obowiązywania Umowy Głównej.
2. A uprawniony jest do rozwiązania Umowy ze skutkiem natychmiastowym w przypadku naruszenia przez B lub jego podmiot przetwarzający postanowień Umowy lub przepisów RODO, lub innych przepisów ochrony danych osobowych, w szczególności, gdy:
   1) organ nadzorczy stwierdzi, że B narusza lub naruszył przepisy RODO,
   2) w wyniku przeprowadzenia audytu A stwierdzi, że B nie przestrzega zasad przetwarzania danych osobowych wynikających z Umowy lub RODO lub innych obowiązujących przepisów prawa.
3. Uprawienie do rozwiązania Umowy ze skutkiem natychmiastowym przysługuje A, choćby naruszenie postanowień Umowy lub przepisów RODO, lub innych przepisów z zakresu ochrony danych osobowych, miało charakter incydentalny.
4. Przez naruszenia B, uprawniające do rozwiązania Umowy ze skutkiem natychmiastowym, należy rozumieć także naruszenia podmiotu przetwarzającego działającego w imieniu lub na rzecz B.

§ 10 Postępowanie z danymi po zakończeniu udostępniania

1. Po zakończeniu udostępniania danych osobowych, niezależnie od sposobu lub przyczyny tego zakończenia, B zobowiązany jest, na swój koszt i ryzyko, do niezwłocznego zwrócenia danych osobowych A i następnie usunięcia wszelkich istniejących ich kopii lub niezwłocznego usunięcia danych osobowych według wyboru A.
2. Dane osobowe lub ich kopie powinny zostać usunięte przez B w terminie 7 dni od dnia zakończenia przetwarzania na podstawie Umowy. B zobowiązany jest do przekazania A w terminie 7 dni od dnia usunięcia danych osobowych, protokołu ich usunięcia.

§ 11 Postanowienia końcowe

1. Wszelkie przesłanki, o których mowa w Umowie mają charakter rozłączny, co oznacza że do nastąpienia skutków prawnych wystarczy spełnienie jednej z nich.
2. Umowa podlega prawu polskiemu.
3. B nie może przenieść praw lub obowiązków wynikających z Umowy bez uprzedniej zgody A, wyrażonej w formie pisemnej pod rygorem nieważności.
4. Umowa uchyla i zastępuje wszelkie postanowienia dotyczące przetwarzania danych osobowych, zawarte uprzednio między Stronami.
5. Wszelkie zmiany lub uzupełnienia Umowy wymagają porozumienia Stron w formie pisemnej pod rygorem nieważności.
6. W przypadku stwierdzenia, że którekolwiek z postanowień Umowy było w momencie jej zawarcia z mocy prawa nieważne lub bezskuteczne, okoliczność ta nie będzie miała wpływu na ważność, skuteczność lub możliwość wyegzekwowania pozostałych jej postanowień. W razie zajścia takiej sytuacji, Strony zobowiązują się zawrzeć aneks do Umowy, na mocy którego zastąpią postanowienia nieważne lub bezskuteczne postanowieniami ważnymi w świetle prawa i w pełni skutecznymi, których cel będzie równoważny lub możliwie najbardziej zbliżony do celu postanowień nieważnych lub bezskutecznych.
7. Wszelkie spory pomiędzy Stronami powstałe w związku z realizacją Umowy, będą rozstrzygane przez sąd właściwy ze względu na siedzibę ….
8. W sprawach nieuregulowanych Umową znajdują zastosowanie przepisy obowiązującego prawa, w szczególności RODO oraz Kodeksu cywilnego.
9. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.
10. Załącznikiem stanowiącym integralną część Umowy jest klauzula informacyjna (art. 14 ust. 1-2 RODO)

…….. ……

(podpis) (podpis)

7.6.2021 PL Dziennik Urzędowy Unii Europejskiej L 199/31

DECYZJA WYKONAWCZA KOMISJI (UE) 2021/914

z dnia 4 czerwca 2021 r.

w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679

(Tekst mający znaczenie dla EOG)

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając 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) ([1]), w szczególności jego art. 28 ust. 7 i art. 46 ust. 2 lit. c),

a także mając na uwadze, co następuje:

(1) Rozwój technologiczny ułatwia transgraniczny przepływ danych, który jest niezbędnym warunkiem rozwoju handlu międzynarodowego i współpracy międzynarodowej. Jednocześnie należy zapewnić, aby w przypadku przekazywania danych osobowych do państw trzecich, w tym w przypadku dalszego przekazywania, nie doszło do obniżenia stopnia ochrony osób fizycznych zagwarantowanego w rozporządzeniu (UE) 2016/679 ([2]). Przepisy dotyczące przekazywania danych zawarte w rozdziale V rozporządzenia (UE) 2016/679 mają zapewnić ciągłość takiego wysokiego stopnia ochrony w przypadku przekazywania danych osobowych do państwa trzeciego ([3]).

(2) Zgodnie z art. 46 ust. 1 rozporządzenia (UE) 2016/679 w razie braku decyzji Komisji na mocy art. 45 ust. 3 stwierdzającej odpowiedni stopień ochrony administrator lub podmiot przetwarzający mogą przekazać dane osobowe do państwa trzeciego wyłącznie, gdy zapewnią odpowiednie zabezpieczenia, i pod warunkiem że obowiązują egzekwowalne prawa osób, których dane dotyczą, i skuteczne środki ochrony prawnej. Takie zabezpieczenia można zapewnić za pomocą standardowych klauzul ochrony danych przyjętych przez Komisję zgodnie z art. 46 ust. 2 lit. c).

(3) Rola standardowych klauzul umownych ogranicza się do zapewnienia odpowiednich zabezpieczeń służących ochronie danych w przypadku międzynarodowego przekazywania danych. Dlatego też administrator lub podmiot przetwarzający przekazujący dane osobowe do państwa trzeciego („podmiot przekazujący dane") i administrator lub podmiot przetwarzający odbierający dane („podmiot odbierający dane") mogą włączać takie standardowe klauzule umowne do szerszej umowy i dodawać inne klauzule lub dodatkowe zabezpieczenia, pod warunkiem że nie są one bezpośrednio lub pośrednio sprzeczne ze standardowymi klauzulami umownymi ani nie naruszają podstawowych praw lub wolności osób, których dane dotyczą. Zachęca się administratorów i podmioty przetwarzające do tego, aby w drodze zobowiązań umownych przewidywali dodatkowe zabezpieczenia stanowiące uzupełnienie standardowych klauzul umownych ([4]). Standardowe klauzule umowne stosuje się bez uszczerbku dla jakichkolwiek zobowiązań umownych podmiotu przekazującego dane lub podmiotu odbierającego dane do zapewnienia poszanowania stosownych przywilejów i immunitetów.

(4) Oprócz zapewniania odpowiednich zabezpieczeń w przypadku przekazywania danych za pomocą standardowych klauzul umownych zgodnie z art. 46 ust. 1 rozporządzenia (UE) 2016/679 podmiot przekazujący dane musi spełnić ogólne obowiązki spoczywające na nim jako na administratorze lub podmiocie przetwarzającym zgodnie z rozporządzeniem (UE) 2016/679. Do takich obowiązków należy między innymi spoczywający na administratorze obowiązek podania osobom, których dane dotyczą, informacji o zamiarze przekazania ich danych osobowych do państwa trzeciego zgodnie z art. 13 ust. 1 lit. f) i art. 14 ust. 1 lit. f) rozporządzenia (UE) 2016/679. W przypadku przekazywania na podstawie art. 46 rozporządzenia (UE) 2016/679 takie informacje muszą obejmować wzmiankę o odpowiednich zabezpieczeniach oraz informację o sposobach uzyskania kopii tych zabezpieczeń lub o miejscu ich udostępnienia.

([1]) Dz.U. L 119 z 4.5.2016, s. 1.
([2]) Art. 44 rozporządzenia (UE) 2016/679.
([3]) Zob. również wyrok Trybunału Sprawiedliwości z dnia 16 lipca 2020 r. w sprawie C-311/18, Data Protection Commissioner/Facebook Ireland Ltd i Maximillian Schrems („Schrems II"), ECLI:EU:C:2020:559, pkt 93.
([4]) Motyw 109 rozporządzenia (UE) 2016/679.

(5) Decyzje Komisji 2001/497/WE ([5]) i 2010/87/UE ([6]) zawierają standardowe klauzule umowne służące ułatwieniu przekazywania danych osobowych przez administratora danych posiadającego jednostkę organizacyjną w Unii administratorowi lub podmiotowi przetwarzającemu mającemu siedzibę w państwie trzecim, które nie zapewnia odpowiedniego stopnia ochrony. Decyzje te wydano na podstawie dyrektywy 95/46/WE Parlamentu Europejskiego i Rady ([7]).

(6) Zgodnie z art. 46 ust. 5 rozporządzenia (UE) 2016/679, decyzja 2001/497/WE i decyzja 2010/87/UE pozostają w mocy do czasu ich zmiany, zastąpienia lub uchylenia w razie potrzeby decyzją Komisji przyjętą na podstawie art. 46 ust. 2 tego rozporządzenia. Standardowe klauzule umowne zawarte w decyzjach wymagały aktualizacji w związku z nowymi wymogami określonymi w rozporządzeniu (UE) 2016/679. Ponadto, odkąd przyjęto te decyzje, w gospodarce cyfrowej nastąpiły istotne zmiany – powszechnie stosuje się nowe i bardziej złożone operacje przetwarzania, często z udziałem wielu podmiotów odbierających dane i podmiotów przekazujących dane, występują długie i złożone łańcuchy przetwarzania, a relacje biznesowe ewoluują. W związku z powyższym konieczne jest zmodernizowanie standardowych klauzul umownych w celu lepszego odzwierciedlenia takich realiów przez uwzględnienie dodatkowych sytuacji przetwarzania i przekazywania oraz w celu umożliwienia stosowania bardziej elastycznego podejścia, na przykład jeżeli chodzi o liczbę stron mogących przystąpić do umowy.

(7) Administrator lub podmiot przetwarzający mogą stosować standardowe klauzule umowne określone w załączniku do niniejszej decyzji, aby zapewnić odpowiednie zabezpieczenia w rozumieniu art. 46 ust. 1 rozporządzenia (UE) 2016/679 na potrzeby przekazywania danych osobowych podmiotowi przetwarzającemu lub administratorowi posiadającemu jednostkę organizacyjną w państwie trzecim, bez uszczerbku dla wykładni pojęcia „międzynarodowego przekazywania danych" w rozporządzeniu (UE) 2016/679. Standardowe klauzule umowne można stosować wyłącznie w odniesieniu do takiego przekazywania danych w zakresie, w jakim przetwarzanie danych przez podmiot odbierający dane nie jest objęte zakresem stosowania rozporządzenia (UE) 2016/679. Dotyczy to również przekazywania danych osobowych przez administratora lub podmiot przetwarzający, którzy nie posiadają jednostki organizacyjnej w Unii, w zakresie, w jakim przetwarzanie podlega rozporządzeniu (UE) 2016/679 zgodnie z jego art. 3 ust. 2, gdyż wiąże się ono z oferowaniem towarów lub usług osobom, których dane dotyczą, w Unii lub z monitorowaniem ich zachowania, o ile do zachowania tego dochodzi w Unii.

(8) Mając na uwadze ogólne dostosowanie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 i rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 ([8]), powinna istnieć możliwość stosowania standardowych klauzuli umownych również w kontekście umowy, o której mowa w art. 29 ust. 4 rozporządzenia (UE) 2018/1725, w odniesieniu do przekazywania danych osobowych podwykonawcy przetwarzania w państwie trzecim przez podmiot przetwarzający, który nie jest instytucją ani organem Unii, ale podlega rozporządzeniu (UE) 2016/679 i przetwarza dane osobowe w imieniu instytucji lub organu Unii zgodnie z art. 29 rozporządzenia (UE) 2018/1725. Zgodność z art. 29 ust. 4 rozporządzenia (UE) 2018/1725 będzie zapewniona, jeżeli umowa odzwierciedla takie same obowiązki ochrony danych jak 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, w szczególności obowiązek zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych pozwalających zapewnić, aby przetwarzanie odpowiadało wymogom określonym w tym rozporządzeniu. Będzie to dotyczyło w szczególności sytuacji, gdy administrator i podmiot przetwarzający korzystają ze standardowych klauzulach umownych zawartych w decyzji wykonawczej Komisji w sprawie standardowych klauzul umownych między administratorami a podmiotami przetwarzającymi dotyczących kwestii, o których mowa w art. 28 ust. 7 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 i art. 29 ust. 7 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 ([9]).

(9) Jeżeli przetwarzanie wiąże się z przekazywaniem danych przez administratorów podlegających rozporządzeniu (UE) 2016/679 podmiotom przetwarzającym nieobjętym terytorialnym zakresem stosowania rozporządzenia lub przez podmioty przetwarzające podlegające rozporządzeniu (UE) 2016/679 podwykonawcom przetwarzania nieobjętym terytorialnym zakresem stosowania rozporządzenia, standardowe klauzule umowne określone w załączniku do niniejszej decyzji również powinny umożliwiać spełnienie wymogów określonych w art. 28 ust. 3 i 4 rozporządzenia (UE) 2016/679.

(10) Standardowe klauzule umowne określone w załączniku do niniejszej decyzji łączą klauzule ogólne z podejściem modułowym, aby uwzględnić różne scenariusze przekazywania danych i złożoność współczesnych łańcuchów przetwarzania. Oprócz klauzul ogólnych administratorzy i podmioty przetwarzające powinni wybrać moduł mający zastosowanie do ich sytuacji, aby dostosować obowiązki spoczywające na nich na mocy standardowych klauzul

([5]) Decyzja Komisji 2001/497/WE 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).

([6]) Decyzja Komisji 2010/87/UE 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).

([7]) 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).

([8]) 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); zob. motyw 5.

([9]) C(2021) 3701.

umownych do roli i obowiązków, jakie pełnią w związku z przedmiotowym przetwarzaniem danych. Należy zapewnić możliwość przestrzegania standardowych klauzul umownych przez więcej niż dwie strony. Ponadto należy zapewnić, aby do standardowych klauzul umownych mogli przystępować dodatkowi administratorzy i dodatkowe podmioty przetwarzające w roli podmiotów przekazujących dane lub podmiotów odbierających dane w całym okresie obowiązywania umowy, której te klauzule są częścią.

(11) W celu ustanowienia odpowiednich zabezpieczeń w standardowych klauzulach umownych należy zapewnić, aby stopień ochrony danych osobowych przekazywanych na ich podstawie był merytorycznie równoważny stopniowi gwarantowanemu w Unii ([10]). Aby zapewnić przejrzystość przetwarzania, osoby, których dane dotyczą, powinny otrzymać kopię standardowych klauzul umownych i zostać poinformowane w szczególności o kategoriach przetwarzanych danych osobowych, prawie do uzyskania kopii standardowych klauzul umownych oraz o wszelkim dalszym przekazywaniu. Dalsze przekazywanie przez podmiot odbierający dane do strony trzeciej w innym państwie trzecim powinno być dopuszczalne wyłącznie w sytuacji, w której taka strona trzecia przystępuje do standardowych klauzul umownych lub w której ciągłość ochrony zapewniono w inny sposób, lub też w określonych sytuacjach, na przykład w przypadku udzielenia przez osobę, której dane dotyczą, wyraźnej, świadomej zgody.

(12) Z pewnymi wyjątkami – w szczególności z wyjątkiem określonych obowiązków dotyczących wyłącznie relacji między podmiotem przekazującym dane a podmiotem odbierającym dane – osoby, których dane dotyczą, powinny mieć możliwość powołania się na standardowe klauzule umowne – i w razie potrzeby ich wyegzekwowania – jako osoby trzecie, na rzecz których zawarto umowę. Dlatego też, o ile strony powinny mieć możliwość wybrania prawa jednego z państw członkowskich jako prawa właściwego dla danych standardowych klauzul umownych, o tyle prawo takie musi dopuszczać możliwość wykonania praw przewidzianych w klauzuli na rzecz osoby trzeciej. Aby istniała możliwość indywidualnego dochodzenia roszczeń, w standardowych klauzulach umownych należy zobowiązać podmiot odbierający dane do poinformowania osób, których dane dotyczą, o punkcie kontaktowym oraz do szybkiego rozpatrywania wszelkich skarg lub żądań. W przypadku sporu między podmiotem odbierającym dane a osobą, której dane dotyczą i która powołuje się na przysługujące jej prawa jako osoba trzecia, na rzecz której zawarto umowę, takiej osobie powinno przysługiwać prawo wniesienia skargi do właściwego organu nadzorczego lub skierowania sporu do rozpatrzenia przez sądy właściwe w UE.

(13) Aby zapewnić skuteczne egzekwowanie, od podmiotu odbierającego dane należy wymagać podporządkowania się właściwości takiego organu i takich sądów oraz zobowiązania się do przestrzegania każdej wiążącej decyzji wydanej na mocy mającego zastosowanie prawa państwa członkowskiego. W szczególności podmiot odbierający dane powinien wyrazić zgodę na odpowiadanie na zapytania, poddawanie się audytom i przestrzeganie środków przyjętych przez organ nadzorczy, w tym środków zaradczych i kompensacyjnych. Dodatkowo podmiot odbierający dane powinien móc zaproponować osobom, których dane dotyczą, możliwość nieodpłatnego dochodzenia roszczeń przed niezależnym organem rozstrzygania sporów. Zgodnie z art. 80 ust. 1 rozporządzenia (UE) 2016/679 osoby, których dane dotyczą, powinny mieć prawo, jeżeli wyrażą taką wolę, do umocowania organizacji lub innych podmiotów do ich reprezentowania w sporach z podmiotem odbierającym dane.

(14) W standardowych klauzulach umownych należy określić postanowienia dotyczące odpowiedzialności między stronami i odpowiedzialności wobec osób, których dane dotyczą, a także postanowienia dotyczące wzajemnego zwrotu kosztów między stronami. Jeżeli osoba, której dane dotyczą, poniosła szkodę majątkową lub niemajątkową w wyniku dowolnego naruszenia określonych w standardowych klauzulach umownych praw osoby trzeciej, na rzecz której zawarto umowę, osoba taka powinna mieć prawo do odszkodowania. Powinno to pozostawać bez uszczerbku dla wszelkiego rodzaju odpowiedzialności określonej w rozporządzeniu (UE) 2016/679.

(15) W przypadku przekazywania podmiotowi odbierającemu dane występującemu w charakterze podmiotu przetwarzającego lub podwykonawcy przetwarzania powinny mieć zastosowanie szczegółowe wymogi zgodnie z art. 28 ust. 3 rozporządzenia (UE) 2016/679. W standardowych klauzulach umownych należy zobowiązać podmiot odbierający dane do udostępnienia wszelkich informacji niezbędnych do wykazania spełnienia obowiązków określonych w tych klauzulach oraz do umożliwienia przeprowadzania audytów jego czynności przetwarzania przez podmiot przekazujący dane i do wniesienia wkładu w te audyty. Jeżeli chodzi o zaangażowanie przez podmiot odbierający dane jakiegokolwiek podwykonawcy przetwarzania, zgodnie z art. 28 ust. 2 i 4 rozporządzenia (UE) 2016/679, w standardowych klauzulach umownych należy w szczególności określić procedurę uzyskania ogólnej lub szczegółowej zgody podmiotu przekazującego dane, a także wymóg zawarcia z podwykonawcą przetwarzania pisemnej umowy zapewniającej stopień ochrony odpowiadający stopniowi ochrony zagwarantowanemu w tych klauzulach.

(16) W standardowych klauzulach umownych należy zapewnić odrębne zabezpieczenia dotyczące szczególnej sytuacji, w której podmiot przetwarzający w Unii przekazuje dane osobowe ich administratorowi w państwie trzecim, i odzwierciedlić określone w rozporządzeniu (UE) 2016/679 ograniczone odrębne obowiązki podmiotów przetwarzających. W szczególności w standardowych klauzulach umownych należy zobowiązać podmiot przetwarzający do poinformowania administratora w sytuacji, gdy podmiot przetwarzający nie jest w stanie zastosować się do jego polecenia, w tym jeżeli takie polecenie narusza unijne prawo ochrony danych, oraz zobowiązać administratora do zaniechania wszelkich działań, które uniemożliwiłyby podmiotowi przetwarzającemu spełnienie spoczywających na nim obowiązków określonych w rozporządzeniu (UE) 2016/679. W klauzulach tych należy również zobowiązać strony do udzielania sobie wzajemnej pomocy w odpowiadaniu na zapytania i żądania ze strony osób, których dane

([10]) Schrems II, pkt 96 i 103. Zob. również motywy 108 i 114 rozporządzenia (UE) 2016/679.

dotyczą, zgodnie z lokalnym prawem, któremu podlega podmiot odbierający dane, lub – w przypadku przetwarzania danych w Unii – zgodnie z rozporządzeniem (UE) 2016/679. Jeżeli unijny podmiot przetwarzający łączy dane osobowe otrzymane od administratora w państwie trzecim z danymi osobowymi zgromadzonymi przez siebie w Unii, zastosowanie powinny mieć dodatkowe wymogi, aby uwzględnić ewentualny wpływ stosowania prawa państwa trzeciego przeznaczenia na przestrzeganie klauzul przez administratora, w szczególności wymogi określające sposób postępowania w sytuacji, w której organy publiczne w państwie trzecim przedstawiają wiążące żądania ujawnienia przekazywanych danych osobowych. Z kolei wszelkie tego typu wymogi są nieuzasadnione, jeżeli outsourcing polega wyłącznie na przetwarzaniu i przekazywaniu z powrotem danych osobowych otrzymanych od administratora i jeżeli działalność ta w każdym przypadku podlega i będzie podlegać jurysdykcji danego państwa trzeciego.

(17) Strony powinny być w stanie wykazać przestrzeganie standardowych klauzul umownych. W szczególności podmiot odbierający dane powinien być zobowiązany do przechowywania odpowiedniej dokumentacji dotyczącej czynności przetwarzania, za które ponosi odpowiedzialność, oraz do niezwłocznego poinformowania podmiotu przekazującego dane, jeżeli z jakiegokolwiek powodu nie jest w stanie zapewnić przestrzegania postanowień klauzul. Z kolei podmiot przekazujący dane powinien zawiesić przekazywanie danych, a w szczególnie poważnych przypadkach jest uprawniony do rozwiązania umowy – o ile problem dotyczy przetwarzania danych osobowych na podstawie standardowych klauzul umownych – jeżeli podmiot odbierający dane narusza klauzule lub nie jest w stanie zapewnić ich przestrzegania. W sytuacji, w której lokalne prawo ma wpływ na przestrzeganie klauzul, powinny mieć zastosowanie przepisy szczególne. Dane osobowe przekazane przed rozwiązaniem umowy i wszelkie ich kopie powinny zostać – w zależności od wyboru dokonanego przez podmiot przekazujący dane – zwrócone temu podmiotowi lub zniszczone.

(18) W standardowych klauzulach umownych należy określić szczególne zabezpieczenia, w szczególności w świetle orzecznictwa Trybunał Sprawiedliwości ([11]), aby uwzględnić ewentualny wpływ stosowania prawa państwa trzeciego przeznaczenia na przestrzeganie tych klauzul przez podmiot odbierający dane, a w szczególności należy określić sposób postępowania w sytuacji, w której organy publiczne w tym państwie przedstawiają wiążące żądania ujawnienia przekazywanych danych osobowych.

(19) Przekazywanie i przetwarzanie danych osobowych na podstawie standardowych klauzul umownych nie powinno mieć miejsca, gdy przepisy i praktyki obowiązujące w państwie trzecim przeznaczenia uniemożliwiają podmiotowi odbierającemu dane przestrzeganie tych klauzul. W tym kontekście za sprzeczne ze standardowymi klauzulami umownymi nie należy uznawać przepisów i praktyk, które nie naruszają istoty podstawowych praw i wolności oraz nie wykraczają poza to, co jest w demokratycznym społeczeństwie środkiem niezbędnym i proporcjonalnym służącym zabezpieczeniu jednego z celów wymienionych w art. 23 ust. 1 rozporządzenia (UE) 2016/679. Strony powinny zagwarantować, że w chwili akceptowania standardowych klauzul umownych nie mają żadnych powodów, aby sądzić, iż przepisy i praktyki mające zastosowanie wobec podmiotu odbierającego dane są niezgodne z tymi wymogami.

(20) Strony powinny przede wszystkim uwzględnić konkretne okoliczności przekazywania danych (takie jak treść i okres obowiązywania umowy, charakter danych, które mają być przekazywane, rodzaj odbiorcy, cel przetwarzania), przepisy i praktyki państwa trzeciego przeznaczenia istotne z punktu widzenia okoliczności przekazywania danych oraz wszelkie zabezpieczenia wprowadzone jako uzupełnienie zabezpieczeń określonych w standardowych klauzulach umownych (w tym stosowne środki umowne, techniczne i organizacyjne mające zastosowanie do przekazywania danych osobowych i przetwarzania tych danych w państwie przeznaczenia). Jeżeli chodzi o wpływ takich przepisów i praktyk na zgodność ze standardowymi klauzulami umownymi, w ogólnej ocenie można wziąć pod uwagę różne elementy, między innymi wiarygodne informacje na temat stosowania prawa w praktyce (w tym orzecznictwo i sprawozdania sporządzone przez niezależne organy nadzoru), występowanie lub brak żądań w tym samym sektorze oraz – wyłącznie w ściśle określonych okolicznościach – udokumentowane praktyczne doświadczenie podmiotu przekazującego dane lub podmiotu odbierającego dane.

(21) Jeżeli po zaakceptowaniu standardowych klauzul umownych podmiot odbierający dane ma powody, aby sądzić, że nie jest w stanie zapewnić przestrzegania tych klauzul, powinien powiadomić o tym podmiot przekazujący dane. Jeżeli podmiot przekazujący dane otrzyma takie powiadomienie lub w inny sposób dowie się, że podmiot odbierający dane nie jest już w stanie zapewnić przestrzegania standardowych klauzul umownych, powinien określić odpowiednie środki w celu zaradzenia tej sytuacji, w razie potrzeby w porozumieniu z właściwym organem nadzorczym. Takie środki mogą obejmować dodatkowe środki przyjęte przez podmiot przekazujący dane lub podmiot odbierający dane, takie jak środki techniczne lub organizacyjne służące zapewnieniu bezpieczeństwa i poufności. Podmiot przekazujący dane powinien być zobowiązany do wstrzymania przekazywania danych, jeżeli uzna, że zapewnienie odpowiednich zabezpieczeń jest niemożliwe, lub na polecenie właściwego organu nadzorczego.

([11]) Schrems II.

(22) W stosownych przypadkach podmiot odbierający dane powinien powiadomić podmiot przekazujący dane i osobę, której dane dotyczą, o otrzymaniu od organu publicznego (w tym sądowego) – zgodnie z przepisami państwa przeznaczenia – prawnie wiążącego żądania ujawnienia danych osobowych przekazywanych na podstawie standardowych klauzul umownych. Takie powiadomienie należy również wystosować w przypadku, gdy podmiot odbierający dane dowie się o jakimkolwiek przypadku bezpośredniego dostępu przez organy publiczne do danych osobowych zgodnie z przepisami państwa trzeciego przeznaczenia. Jeżeli podmiot odbierający dane, mimo dołożenia wszelkich starań, nie jest w stanie powiadomić podmiotu przekazującego dane lub osoby, której dane dotyczą, o konkretnych żądaniach ujawnienia danych, powinien dostarczyć podmiotowi przekazującemu dane jak najwięcej istotnych informacji o tych żądaniach. Ponadto podmiot odbierający dane powinien w regularnych odstępach czasu przekazywać podmiotowi przekazującemu dane informacje zbiorcze. Podmiot odbierający dane powinien być również zobowiązany do udokumentowania każdego otrzymanego żądania ujawnienia danych i udzielonej odpowiedzi oraz udostępnienia tych informacji podmiotowi przekazującemu dane lub właściwemu organowi nadzorczemu, lub obu tym podmiotom, na ich wniosek. Jeżeli po zbadaniu zgodności takiego żądania z prawem państwa przeznaczenia podmiot odbierający dane dojdzie do wniosku, że istnieją uzasadnione podstawy, by uznać, że żądanie jest niezgodne z prawem w świetle prawa państwa trzeciego przeznaczenia, powinien zaskarżyć takie żądanie, w tym, w stosownych przypadkach, poprzez wyczerpanie dostępnych środków odwoławczych. Niezależnie od sytuacji, jeżeli podmiot odbierający dane nie jest już w stanie zapewnić przestrzegania standardowych klauzul umownych, powinien powiadomić o tym podmiot przekazujący dane, w tym jeżeli jest to skutkiem żądania ujawnienia danych.

(23) Ponieważ potrzeby, technologia i operacje przetwarzania zainteresowanych stron mogą się zmieniać, Komisja powinna ocenić funkcjonowanie standardowych klauzul umownych na podstawie zdobytych doświadczeń w ramach okresowej oceny rozporządzenia (UE) 2016/679, o której mowa w art. 97 tego rozporządzenia.

(24) Decyzję 2001/497/WE oraz decyzję 2010/87/UE należy uchylić trzy miesiące po wejściu w życie niniejszej decyzji. W tym okresie podmioty przekazujące dane i podmioty odbierające dane powinny, do celów art. 46 ust. 1 rozporządzenia (UE) 2016/679, nadal mieć możliwość stosowania standardowych klauzul umownych określonych w decyzjach 2001/497/WE i 2010/87/UE. Przez dodatkowy okres 15 miesięcy podmioty przekazujące dane i podmioty odbierające dane powinny, do celów art. 46 ust. 1 rozporządzenia (UE) 2016/679, mieć możliwość dalszego stosowania standardowych klauzul umownych określonych w decyzjach 2001/497/WE i 2010/87/UE w odniesieniu do wykonywania umów zawartych między nimi przed datą uchylenia tych decyzji, pod warunkiem że operacje przetwarzania będące przedmiotem umowy pozostaną niezmienione i pod warunkiem że stosowanie tych klauzul zapewnia, aby przekazywanie danych osobowych odbywało się z zastrzeżeniem odpowiednim zabezpieczeń w rozumieniu art. 46 ust. 1 rozporządzenia (UE) 2016/679. W przypadku istotnych zmian w umowie podmiot przekazujący dane powinien być zobowiązany do oparcia się na nowej podstawie przekazywania danych na mocy umowy, w szczególności poprzez zastąpienie istniejących standardowych klauzul umownych standardowymi klauzulami umownymi określonymi w załączniku do niniejszej decyzji. To samo powinno mieć zastosowanie do wszelkich przypadków zlecania podmiotowi przetwarzającemu (podwykonawcy przetwarzania) podwykonawstwa operacji przetwarzania objętych umową.

(25) Zgodnie z art. 42 ust. 1 i 2 rozporządzenia (UE) 2018/1725 skonsultowano się z Europejskim Inspektorem Ochrony Danych i Europejską Radą Ochrony Danych – w dniu 14 stycznia 2021 r. organy te wydały wspólną opinię ([12]), którą uwzględniono podczas przygotowywania niniejszej decyzji.

(26) Środki przewidziane w niniejszej decyzji są zgodne z opinią komitetu ustanowionego na mocy art. 93 rozporządzenia (UE) 2016/679,

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

Artykuł 1

1. 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 przez administratora lub podmiot przetwarzający danych osobowych przetwarzanych zgodnie z tym rozporządzeniem (podmiot przekazujący dane) administratorowi lub podmiotowi przetwarzającemu (podwykonawcy przetwarzania), w przypadku których przetwarzanie danych nie podlega temu rozporządzeniu (podmiot odbierający dane).

2. Standardowe klauzule umowne określają również prawa i obowiązki administratorów i podmiotów przetwarzających w odniesieniu do kwestii, o których mowa w art. 28 ust. 3 i 4 rozporządzenia (UE) 2016/679, jeżeli chodzi o przekazywanie danych osobowych przez administratora podmiotowi przetwarzającemu lub przez podmiot przetwarzający podwykonawcy przetwarzania.

([12]) Wspólna opinia EROD-EIOD 2/2021 dotycząca decyzji wykonawczej Komisji Europejskiej w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich w odniesieniu do kwestii, o których mowa w art. 46 ust. 2 lit. c) rozporządzenia (UE) 2016/679.

Artykuł 2

Jeżeli właściwe organy państwa członkowskiego wykonują uprawnienia naprawcze na podstawie art. 58 rozporządzenia (UE) 2016/679 w odpowiedzi na fakt, że podmiot odbierający dane podlega lub zaczął podlegać w państwie trzecim przeznaczenia przepisom lub praktykom, które uniemożliwiają mu przestrzeganie standardowych klauzul umownych określonych w załączniku, co prowadzi do wstrzymania lub zakazu przekazywania danych do państw trzecich, przedmiotowe państwo członkowskie niezwłocznie informuje o tym Komisję, która przekazuje te informacje pozostałym państwom członkowskim.

Artykuł 3

Komisja ocenia praktyczne stosowanie standardowych klauzul umownych określonych w załączniku na podstawie wszystkich dostępnych informacji, w ramach okresowej oceny wymaganej zgodnie z art. 97 rozporządzenia (UE) 2016/679.

Artykuł 4

1. Niniejsza decyzja wchodzi w życie dwudziestego dnia po jej opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

2. Decyzja 2001/497/WE traci moc ze skutkiem od dnia 27 września 2021 r.

3. Decyzja 2010/87/UE traci moc ze skutkiem od dnia 27 września 2021 r.

4. Uznaje się, że umowy zawarte przed dniem 27 września 2021 r. na podstawie decyzji 2001/497/WE lub decyzji 2010/87/UE zapewniają odpowiednie gwarancje w rozumieniu art. 46 ust. 1 rozporządzenia (UE) 2016/679 do dnia 27 grudnia 2022 r., pod warunkiem że operacje przetwarzania stanowiące przedmiot umowy pozostaną niezmienione oraz że stosowanie tych klauzul zapewnia, aby przekazywanie danych osobowych odbywało się z zastrzeżeniem odpowiednich zabezpieczeń.

Sporządzono w Brukseli dnia 4 czerwca 2021 r.

W imieniu Komisji
Ursula VON DER LEYEN
Przewodnicząca

ZAŁĄCZNIK

STANDARDOWE KLAUZULE UMOWNE

SEKCJA I

Klauzula 1

Cel i zakres

a) Niniejsze standardowe klauzule umowne mają na celu zapewnienie zgodności z wymogami 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 (ogólne rozporządzenie o ochronie danych) ([1]) w zakresie przekazywania danych osobowych do państwa trzeciego.

b) Strony:

(i) osoby fizyczne lub prawne, organy publiczne, agencje lub inne organy (zwane dalej „podmiotami") przekazujące dane osobowe, wymienione w załączniku I część A (zwane dalej „podmiotem przekazującym dane") oraz

(ii) podmioty w państwie trzecim otrzymujące dane osobowe od podmiotu przekazującego dane, bezpośrednio lub pośrednio za pośrednictwem innego podmiotu, będącego również Stroną niniejszych klauzul, umieszczone w wykazie w załączniku I część A (zwane dalej „podmiotem odbierającym dane")

uzgodniły niniejsze standardowe klauzule umowne (zwane dalej „klauzulami").

c) Niniejsze klauzule mają zastosowanie do przekazywania danych osobowych, jak określono w załączniku I część B.

d) Dodatek do niniejszych klauzul zawierający wymienione w nich załączniki stanowi integralną część niniejszych klauzul.

Klauzula 2

Skutek i niezmienność klauzul

a) Niniejsze klauzule określają odpowiednie zabezpieczenia, w tym egzekwowalne prawa osób, których dane dotyczą, i skuteczne środki ochrony prawnej, zgodnie z art. 46 ust. 1 i art. 46 ust. 2 lit. c) rozporządzenia (UE) 2016/679, oraz standardowe klauzule umowne zgodnie z art. 28 ust. 7 rozporządzenia (UE) 2016/679 w odniesieniu do przekazywania danych od administratorów do podmiotów przetwarzających lub od podmiotów przetwarzających do podmiotów przetwarzających, pod warunkiem że klauzule te nie są modyfikowane, z wyjątkiem modyfikowania w celu wyboru odpowiedniego modułu lub odpowiednich modułów lub w celu dodania informacji do dodatku lub aktualizacji takich informacji. Nie uniemożliwia to Stronom włączania standardowych klauzul umownych określonych w niniejszych klauzulach do szerszej umowy lub dodawania innych klauzul lub dodatkowych zabezpieczeń, pod warunkiem że nie są one bezpośrednio ani pośrednio sprzeczne z niniejszymi klauzulami ani nie naruszają podstawowych praw lub wolności osób, których dane dotyczą.

b) Niniejsze klauzule nie naruszają obowiązków, którym podlega podmiot przekazujący dane na mocy rozporządzenia (UE) 2016/679.

Klauzula 3

Osoby trzecie, na rzecz których zawarto umowę

a) Osoby, których dane dotyczą, mogą powoływać się na niniejsze klauzule i egzekwować je, jako osoby trzecie, na rzecz których zawarto umowę, względem podmiotu przekazującego dane lub podmiotu odbierającego dane, z następującymi wyjątkami:

(i) klauzula 1, klauzula 2, klauzula 3, klauzula 6, klauzula 7;

([1]) Gdy podmiot przekazujący dane jest podmiotem przetwarzającym podlegającym rozporządzeniu (UE) 2016/679, działającym w imieniu instytucji lub organu Unii, poleganie na niniejszych klauzulach przy angażowaniu innego podmiotu przetwarzającego (podwykonawstwo przetwarzania) niepodlegającego rozporządzeniu (UE) 2016/679 zapewnia również zgodność z art. 29 ust. 4 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 oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE (Dz.U. L 295 z 21.11.2018, s. 39) w zakresie, w jakim niniejsze klauzule oraz obowiązki dotyczące ochrony danych, określone w umowie lub innym akcie prawnym zawartym między administratorem a podmiotem przetwarzającym zgodnie z art. 29 ust. 3 rozporządzenia (UE) 2018/1725, są ze sobą zgodne. Będzie to dotyczyło w szczególności sytuacji, gdy administrator i podmiot przetwarzający opierają się na standardowych klauzulach umownych zawartych w decyzji 2021/915

(ii) klauzula 8 – moduł pierwszy: klauzula 8.5 lit. e) i klauzula 8.9 lit. b); moduł drugi: klauzula 8.1 lit. b), klauzula 8.9 lit. a), c), d) i e); moduł trzeci: klauzula 8.1 lit. a), c) i d) oraz klauzula 8.9 lit. a), c), d), e), f) i g); moduł czwarty: klauzula 8.1 lit. b) oraz klauzula 8.3 lit. b);

(iii) klauzula 9 – moduł drugi: klauzula 9 lit. a), c), d) i e); moduł trzeci: klauzula 9 lit. a), c), d) i e);

(iv) klauzula 12 – moduł pierwszy: klauzula 12 lit. a) i d); moduły drugi i trzeci: klauzula 12 lit. a), d) i f);

(v) klauzula 13;

(vi) klauzula 15.1 lit. c), d) i e);

(vii) klauzula 16 lit. e);

(viii) klauzula 18 – moduły pierwszy, drugi i trzeci: klauzula 18 lit. a) i b); moduł czwarty: klauzula 18.

b) Lit. a) pozostaje bez uszczerbku dla praw osób, których dane dotyczą, w trybie rozporządzenia (UE) 2016/679.

Klauzula 4

Interpretacja

a) W przypadku gdy w niniejszych klauzulach stosuje się terminy zdefiniowane w rozporządzeniu (UE) 2016/679, terminy te mają znaczenie nadane im w tym rozporządzeniu.

b) Niniejsze klauzule należy odczytywać i interpretować w świetle przepisów rozporządzenia (UE) 2016/679.

c) Klauzul tych nie należy interpretować w sposób sprzeczny z prawami i obowiązkami określonymi w rozporządzeniu (UE) 2016/679.

Klauzula 5

Hierarchia

W przypadku sprzeczności między niniejszymi klauzulami a postanowieniami powiązanych umów między Stronami, obowiązujących w chwili uzgodnienia niniejszych klauzul, lub zawartych w późniejszym terminie, niniejsze klauzule mają pierwszeństwo.

Klauzula 6

Opis przekazywania danych

Szczegóły dotyczące przekazywania danych, w szczególności kategorie przekazywanych danych osobowych oraz cel lub cele ich przekazywania, określono w załączniku I część B.

Klauzula 7 – Nieobowiązkowa

Klauzula przystąpienia

a) Podmiot, który nie jest Stroną niniejszych klauzul, może za zgodą Stron przystąpić do tych klauzul w dowolnym momencie albo jako podmiot przekazujący dane, albo jako podmiot odbierający dane, wypełniając dodatek i podpisując załącznik I część A.

b) Po wypełnieniu dodatku i podpisaniu załącznika I część A podmiot przystępujący staje się Stroną niniejszych klauzul oraz nabywa prawa i obowiązki podmiotu przekazującego dane lub podmiotu odbierającego dane, zgodnie z jego określeniem w załączniku I część A.

c) Podmiot przystępujący nie ma żadnych praw ani obowiązków wynikających z niniejszych klauzul w odniesieniu do okresu, zanim został ich Stroną.

SEKCJA II – OBOWIĄZKI STRON

Klauzula 8

Zabezpieczenia służące ochronie danych

Podmiot przekazujący dane gwarantuje, że dołożył zasadnych starań w celu ustalenia, że podmiot odbierający dane jest w stanie – dzięki wdrożeniu odpowiednich środków technicznych i organizacyjnych – wypełnić swoje obowiązki określone w niniejszych klauzulach.

MODUŁ PIERWSZY: Przekazywanie między administratorami

8.1. **Ograniczenie celu**

Podmiot odbierający dane przetwarza dane osobowe wyłącznie w określonym celu lub określonych celach przekazywania, jak wskazano w załączniku I część B. Może on przetwarzać dane osobowe w innym celu wyłącznie w przypadku:

(i) uzyskania uprzedniej zgody osoby, której dane dotyczą;

(ii) gdy jest to niezbędne do ustalenia, dochodzenia lub obrony roszczeń w kontekście szczególnego postępowania administracyjnego, regulacyjnego lub sądowego; lub

(iii) gdy jest to niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej.

8.2. **Przejrzystość**

a) W celu umożliwienia osobom, których dane dotyczą, skutecznego wykonywania ich praw zgodnie z klauzulą 10, podmiot odbierający dane przekazuje im, bezpośrednio lub za pośrednictwem podmiotu przekazującego dane, informacje dotyczące:

(i) swoich danych identyfikujących i danych kontaktowych;

(ii) kategorii przetwarzanych danych osobowych;

(iii) prawa do otrzymania kopii niniejszych klauzul;

(iv) w przypadku gdy planuje dalsze przekazywanie danych osobowych stronie trzeciej lub stronom trzecim – odbiorcy lub kategorii odbiorców (w razie potrzeby w celu przekazania istotnych informacji), celu dalszego przekazania oraz jego uzasadnienia zgodnie z klauzulą 8.7.

b) Lit. a) nie ma zastosowania w przypadku, gdy osoba, której dane dotyczą, już posiada te informacje, w tym gdy podmiot przekazujący dane przekazał już te informacje lub przekazanie ich jest niemożliwe lub wymagałoby niewspółmiernego wysiłku ze strony podmiotu odbierającego dane. W tym drugim przypadku podmiot odbierający dane udostępnia publicznie dane w zakresie, w jakim jest to możliwe.

c) Strony udostępniają bezpłatnie na żądanie osobie, której dane dotyczą, kopię niniejszych klauzul, w tym dodatek wypełniony przez Strony. W zakresie koniecznym w celu ochrony tajemnic handlowych lub innych informacji poufnych, w tym danych osobowych, Strony mogą częściowo zredagować tekst dodatku przed udostępnieniem jego kopii, lecz przekazują stosowne streszczenie, jeżeli bez takiego streszczenia osoba, której dane dotyczą, nie byłaby w stanie zrozumieć treści takiego tekstu lub korzystać ze swoich praw. Na żądanie Strony przekazują osobie, której dane dotyczą, powody zredagowania tekstu, w miarę możliwości bez ujawniania utajnionych informacji.

d) Postanowienia zawarte w lit. a)–c) pozostają bez uszczerbku dla obowiązków spoczywających na podmiocie przekazującym dane na mocy art. 13 i 14 rozporządzenia (UE) 2016/679.

8.3. **Prawidłowość i minimalizacja danych**

a) Każda Strona zapewnia, aby dane osobowe były prawidłowe i w razie potrzeby uaktualniane. Podmiot odbierający dane podejmuje wszelkie zasadne działania, aby dane osobowe, które są nieprawidłowe w świetle celu lub celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane.

b) Jeżeli jedna ze Stron zda sobie sprawę, że przekazane lub otrzymane przez nią dane osobowe są nieprawidłowe lub nieaktualne, powiadamia o tym bez zbędnej zwłoki drugą Stronę.

c) Podmiot odbierający dane zapewnia, aby dane osobowe były adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celu lub celów przetwarzania.

8.4. **Ograniczenie przechowywania**

Podmiot odbierający dane zatrzymuje dane osobowe przez okres nie dłuższy, niż jest to niezbędne do celu lub celów, w których dane te są przetwarzane. Wdraża on odpowiednie środki techniczne lub organizacyjne, aby zapewnić wypełnienie tego obowiązku, w tym usunięcie lub anonimizację ([2]) danych oraz wszelkich kopii zapasowych po zakończeniu okresu zatrzymywania.

8.5. **Bezpieczeństwo przetwarzania**

a) Podmiot odbierający dane, a podczas przesyłania również podmiot przekazujący dane, wdraża odpowiednie środki techniczne i organizacyjne w celu zapewnienia bezpieczeństwa danych osobowych, w tym ochrony przeciwko naruszeniu bezpieczeństwa prowadzącemu do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu (zwanego dalej „naruszeniem ochrony danych osobowych"). Przy ocenie odpowiedniego poziomu bezpieczeństwa podmioty te uwzględniają stan wiedzy technicznej, koszty wdrażania oraz charakter, zakres, kontekst i cel lub cele przetwarzania, a także ryzyko wynikające z przetwarzania dla osoby, której dane dotyczą. Strony rozważą w szczególności posłużenie się szyfrowaniem lub pseudonimizacją, w tym podczas przesyłania, w przypadkach, gdy cel przetwarzania może być spełniony w ten sposób.

b) Strony uzgodniły środki techniczne i organizacyjne określone w załączniku II. Podmiot odbierający dane przeprowadza regularne kontrole, aby zagwarantować, że środki te wciąż zapewniają odpowiedni poziom bezpieczeństwa.

c) Podmiot odbierający dane zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania poufności lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania poufności.

d) W przypadku naruszenia ochrony danych osobowych dotyczącego danych osobowych przetwarzanych przez podmiot odbierający dane na podstawie niniejszych klauzul podmiot odbierający dane stosuje odpowiednie środki w celu zaradzenia naruszeniu danych osobowych, w tym środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

e) W przypadku naruszenia ochrony danych osobowych, które może powodować ryzyko naruszenia praw i wolności osób fizycznych, podmiot odbierający dane bez zbędnej zwłoki zgłasza takie naruszenie zarówno podmiotowi przekazującemu dane, jak i właściwemu organowi nadzorczemu zgodnie z klauzulą 13. Zgłoszenie takie zawiera: (i) opis charakteru naruszenia (w tym w miarę możliwości kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie), (ii) jego możliwe konsekwencje, (iii) środki zastosowane lub proponowane w celu zaradzenia naruszeniu oraz (iv) szczegółowe dane dotyczące punktu kontaktowego, w którym można uzyskać więcej informacji. W zakresie, w jakim dla podmiotu odbierającego dane niemożliwe jest udzielenie wszystkich informacji w tym samym czasie, może udzielać ich sukcesywnie bez zbędnej zwłoki.

f) W przypadku naruszenia ochrony danych osobowych, które może powodować ryzyko naruszenia praw i wolności osób fizycznych, administrator bez zbędnej zwłoki zgłasza również osobom, których dane dotyczą, naruszenie ochrony danych osobowych oraz jego charakter, w stosownych przypadkach we współpracy z podmiotem przekazującym dane, wraz z informacjami, o których mowa w lit. e) ppkt (ii)–(iv), chyba że podmiot odbierający dane wdrożył środki służące istotnemu ograniczeniu ryzyka naruszenia praw lub wolności osób fizycznych lub zgłoszenie wymagałoby niewspółmiernie dużego wysiłku. W tym drugim przypadku podmiot odbierający dane zamiast tego wydaje komunikat publiczny lub podejmuje podobne działanie w celu poinformowania ogółu społeczeństwa o naruszeniu ochrony danych osobowych.

g) Podmiot odbierający dane dokumentuje wszelkie istotne fakty związane z naruszeniem ochrony danych osobowych, w tym jego skutki oraz wszelkie podjęte działania zaradcze.

8.6. **Dane wrażliwe**

Gdy przekazywanie obejmuje dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne lub dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej tej osoby lub dane dotyczące wyroków skazujących lub czynów zabronionych (zwane dalej „danymi wrażliwymi"), podmiot odbierający dane stosuje szczególne ograniczenia lub dodatkowe zabezpieczenia dostosowane do szczególnego charakteru danych i ponoszonego ryzyka. Mogą one obejmować ograniczenia w zakresie personelu, któremu zezwala się na dostęp do danych osobowych, dodatkowe środki bezpieczeństwa (takie jak pseudonimizacja) lub dodatkowe ograniczenia dotyczące dalszego ujawniania.

([2]) Oznacza to dokonanie anonimizacji danych w taki sposób, aby osób, których dane dotyczą, nie można było zidentyfikować, zgodnie z motywem 26 rozporządzenia (UE) 2016/679, oraz aby proces ten był nieodwracalny.

8.7. **Dalsze przekazywanie danych**

Podmiot odbierający dane nie ujawnia danych osobowych stronie trzeciej zlokalizowanej poza terytorium Unii Europejskiej ([3]) (w tym samym państwie co podmiot odbierający dane lub w innym państwie trzecim; dalej „dalsze przekazanie"), chyba że strona trzecia jest związana niniejszymi klauzulami bądź zgadza się im podlegać, na mocy odpowiedniego modułu. W innych przypadkach dalsze przekazanie przez podmiot odbierający dane może mieć miejsce wyłącznie wówczas, gdy:

(i) odbywa się do państwa objętego decyzją stwierdzającą odpowiedni stopień ochrony, zgodnie z art. 45 rozporządzenia (UE) 2016/679, obejmującą dalsze przekazywanie;

(ii) strona trzecia zapewnia w inny sposób odpowiednie zabezpieczenia w odniesieniu do przedmiotowego przetwarzania zgodnie z art. 46 lub 47 rozporządzenia (UE) 2016/679;

(iii) strona trzecia zawiera wiążący instrument z podmiotem odbierającym dane, zapewniający taki sam poziom ochrony danych jak poziom przewidziany w niniejszych klauzulach, a podmiot odbierający dane przekazuje kopię tych zabezpieczeń podmiotowi przekazującemu dane;

(iv) jest ono niezbędne do ustalenia, dochodzenia lub obrony roszczeń w kontekście szczególnego postępowania administracyjnego, regulacyjnego lub sądowego;

(v) jest ono jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej; lub

(vi) jeżeli żaden z pozostałych warunków nie ma zastosowania – podmiot odbierający dane uzyskał wyraźną zgodę osoby, której dane dotyczą, na dalsze ich przekazywanie w określonej sytuacji, po uprzednim poinformowaniu tej osoby o celu lub celach dalszego przekazania, tożsamości odbiorcy oraz ewentualnym ryzyku, na które – ze względu na brak odpowiednich zabezpieczeń służących ochronie danych – może być narażona osoba, której dane dotyczą, w związku z tym przekazaniem. W takim przypadku podmiot odbierający dane informuje podmiot przekazujący dane i na żądanie tego ostatniego przekazuje mu kopię informacji przekazanych osobie, której dane dotyczą.

Wszelkie dalsze przekazanie odbywa się pod warunkiem przestrzegania przez podmiot odbierający dane wszystkich pozostałych zabezpieczeń na mocy niniejszych klauzul, w szczególności ograniczenia celu.

8.8. **Przetwarzanie z upoważnienia podmiotu odbierającego dane**

Podmiot odbierający dane zapewnia, aby każda osoba działająca z jego upoważnienia, w tym podmiot przetwarzający, przetwarzała dane wyłącznie na jego polecenie.

8.9. **Dokumentacja i zgodność**

a) Każda ze Stron będzie w stanie wykazać, że przestrzega ciążących na niej obowiązków wynikających z niniejszych klauzul. W szczególności podmiot odbierający dane przechowuje odpowiednią dokumentację wykonanych czynności przetwarzania, za które odpowiada.

b) Podmiot odbierający dane udostępnia tę dokumentację na żądanie właściwego organu nadzorczego.

MODUŁ DRUGI: Przekazywanie przez administratora podmiotowi przetwarzającemu

8.1. **Polecenie**

a) Podmiot odbierający dane przetwarza dane osobowe wyłącznie na udokumentowane polecenie podmiotu przekazującego dane. Podmiot przekazujący dane może wydawać takie polecenia w całym okresie obowiązywania umowy.

b) Podmiot odbierający dane niezwłocznie informuje podmiot przekazujący dane, jeżeli nie może wykonać tego polecenia.

8.2. **Ograniczenie celu**

Podmiot odbierający dane przetwarza dane osobowe wyłącznie w określonym celu/określonych celach przekazywania, jak wskazano w załączniku I część B, chyba że działa na podstawie dalszych poleceń wydanych przez podmiot przekazujący dane.

([3]) W Porozumieniu o Europejskim Obszarze Gospodarczym (Porozumienie EOG) przewidziano rozszerzenie rynku wewnętrznego Unii Europejskiej na trzy państwa EOG – Islandię, Liechtenstein i Norwegię. Unijne prawodawstwo dotyczące ochrony danych, w tym rozporządzenie (UE) 2016/679, jest objęte Porozumieniem EOG i zostało włączone do jego załącznika XI. W związku z tym wszelkie ujawnianie danych stronie trzeciej zlokalizowanej w EOG przez podmiot odbierający dane nie kwalifikuje się jako dalsze przekazanie do celów niniejszych klauzul.

8.3. **Przejrzystość**

Podmiot przekazujący dane udostępnia bezpłatnie na żądanie osobie, której dane dotyczą, kopię niniejszych klauzul, w tym dodatku wypełnionego przez Strony. W zakresie koniecznym w celu ochrony tajemnic handlowych lub innych informacji poufnych, w tym środków opisanych w załączniku II i danych osobowych, podmiot przekazujący dane może częściowo zredagować tekst dodatku do tych klauzul przed udostępnieniem jego kopii, lecz przekazuje stosowne streszczenie, jeżeli bez takiego streszczenia osoba, której dane dotyczą, nie byłaby w stanie zrozumieć treści takiego tekstu lub korzystać ze swoich praw. Na żądanie Strony przekazują osobie, której dane dotyczą, powody zredagowania tekstu, w miarę możliwości bez ujawniania utajnionych informacji. Klauzula ta pozostaje bez uszczerbku dla obowiązków spoczywających na podmiocie przekazującym dane na mocy art. 13 i 14 rozporządzenia (UE) 2016/679.

8.4. **Prawidłowość**

Jeżeli podmiot odbierający dane zda sobie sprawę, że otrzymane przez niego dane osobowe są nieprawidłowe lub nieaktualne, powiadamia o tym bez zbędnej zwłoki podmiot przekazujący dane. W takim przypadku podmiot odbierający dane współpracuje z podmiotem przekazującym dane w celu ich usunięcia lub sprostowania.

8.5. **Czas trwania przetwarzania oraz usuwanie lub zwrot danych**

Przetwarzanie danych przez podmiot odbierający dane odbywa się wyłącznie przez czas określony w załączniku I część B. Po zakończeniu świadczenia usług przetwarzania podmiot odbierający dane, zgodnie z wyborem podmiotu przekazującego dane, albo usuwa wszystkie dane osobowe przetworzone w imieniu podmiotu przekazującego dane i potwierdza podmiotowi przekazującemu dane ich usunięcie, albo zwraca podmiotowi przekazującemu dane wszystkie dane osobowe przetworzone w jego imieniu i usuwa istniejące kopie. Do czasu usunięcia lub zwrotu danych podmiot odbierający dane nadal zapewnia zgodność z niniejszymi klauzulami. Jeżeli lokalne prawo obowiązujące podmiot odbierający dane zabrania zwrotu lub usunięcia danych osobowych, podmiot odbierający dane gwarantuje, że będzie w dalszym ciągu zapewniał przestrzeganie niniejszych klauzul oraz że będzie przetwarzał je wyłącznie w zakresie i w czasie wymaganym przez to prawo lokalne. Zasada ta pozostaje bez uszczerbku dla klauzuli 14, w szczególności wymogu określonego w klauzuli 14 lit. e), aby podmiot odbierający dane zgłaszał w okresie obowiązywania umowy podmiotowi przekazującemu dane, jeżeli ma powody, aby sądzić, że podlega lub zaczął podlegać przepisom lub praktykom niezgodnym z wymogami określonymi w klauzuli 14 lit. a).

8.6. **Bezpieczeństwo przetwarzania**

a) Podmiot odbierający dane, a podczas przesyłania również podmiot przekazujący dane, wdraża odpowiednie środki techniczne i organizacyjne w celu zapewnienia bezpieczeństwa danych, w tym ochrony przeciwko naruszeniu bezpieczeństwa prowadzącego do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do tych danych (zwanego dalej „naruszeniem ochrony danych osobowych"). Przy ocenie odpowiedniego poziomu bezpieczeństwa Strony uwzględniają stan wiedzy technicznej, koszty wdrażania oraz charakter, zakres, kontekst i cel lub cele przetwarzania, a także ryzyko wynikające z przetwarzania dla osób, których dane dotyczą. Strony rozważą w szczególności posłużenie się szyfrowaniem lub pseudonimizacją, w tym podczas przesyłania, w przypadkach, gdy cel przetwarzania może być spełniony w ten sposób. W przypadku pseudonimizacji dodatkowe informacje w celu przypisania danych osobowych konkretnej osobie, której dane dotyczą, pozostają, jeżeli jest to możliwe, pod wyłączną kontrolą podmiotu przekazującego dane. W ramach obowiązków w trybie niniejszej litery podmiot odbierający dane wdraża co najmniej środki techniczne i organizacyjne określone w załączniku II. Podmiot odbierający dane przeprowadza regularne kontrole, aby zagwarantować, że środki te wciąż zapewniają odpowiedni poziom bezpieczeństwa.

b) Podmiot odbierający dane udziela dostępu do danych osobowych członkom swojego personelu wyłącznie w zakresie ściśle niezbędnym do wykonywania umowy, zarządzania umową oraz jej monitorowania. Zapewnia on, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania poufności lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania poufności.

c) W przypadku naruszenia ochrony danych osobowych dotyczącego danych osobowych przetwarzanych przez podmiot odbierający dane na podstawie niniejszych klauzul podmiot odbierający dane stosuje odpowiednie środki w celu zaradzenia temu naruszeniu, w tym środki w celu zminimalizowania jego negatywnych skutków. Po stwierdzeniu naruszenia podmiot odbierający dane zgłasza je również bez zbędnej zwłoki podmiotowi przekazującemu dane. Zgłoszenie takie zawiera szczegóły dotyczące punktu kontaktowego, w którym można uzyskać więcej informacji, opis charakteru naruszenia (w tym, gdy jest to możliwe, kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie), jego możliwe konsekwencje oraz środki zastosowane lub proponowane w celu zaradzenia naruszeniu, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków. Jeżeli oraz w zakresie, w jakim niemożliwe jest udzielenie wszystkich informacji w tym samym czasie, pierwotne zgłoszenie zawiera informacje dostępne w danym momencie, a dalszych informacji udziela się sukcesywnie, bez zbędnej zwłoki w miarę, jak staną się one dostępne.

d) Podmiot odbierający dane współpracuje z podmiotem przekazującym dane i pomaga mu, aby umożliwić podmiotowi przekazującemu dane wypełnienie obowiązków określonych w rozporządzeniu (UE) 2016/679, w szczególności obowiązku powiadomienia właściwego organu nadzorczego oraz poszkodowanych osób, których dane dotyczą, uwzględniając charakter przetwarzania oraz informacje, do których podmiot odbierający dane ma dostęp.

8.7. **Dane wrażliwe**

Gdy przekazywanie obejmuje dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne lub dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej tej osoby lub dane dotyczące wyroków skazujących i czynów zabronionych (zwane dalej „danymi wrażliwymi"), podmiot odbierający dane stosuje szczególne ograniczenia lub dodatkowe zabezpieczenia opisane w załączniku I część B.

8.8. **Dalsze przekazywanie danych**

Podmiot odbierający dane ujawnia dane osobowe stronie trzeciej wyłącznie na podstawie udokumentowanego polecenia podmiotu przekazującego dane. Ponadto dane mogą zostać ujawnione stronie trzeciej zlokalizowanej poza terytorium Unii Europejskiej ([4]) (w tym samym państwie co podmiot odbierający dane lub w innym państwie trzecim; dalej „dalsze przekazanie") wyłącznie wówczas, gdy strona trzecia jest związana niniejszymi klauzulami bądź zgadza się im podlegać na mocy odpowiedniego modułu lub jeżeli:

(i) dalsze przekazanie odbywa się do państwa objętego decyzją stwierdzającą odpowiedni stopień ochrony, zgodnie z art. 45 rozporządzenia (UE) 2016/679, obejmującą dalsze przekazywanie;

(ii) strona trzecia zapewnia w inny sposób odpowiednie zabezpieczenia w odniesieniu do przedmiotowego przetwarzania zgodnie z art. 46 lub 47 rozporządzenia (UE) 2016/679;

(iii) dalsze przekazanie jest niezbędne do ustalenia, dochodzenia lub ochrony roszczeń w kontekście szczególnego postępowania administracyjnego, regulacyjnego lub sądowego; lub

(iv) dalsze przekazanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej.

Wszelkie dalsze przekazanie odbywa się pod warunkiem przestrzegania przez podmiot odbierający dane wszystkich pozostałych zabezpieczeń na mocy niniejszych klauzul, w szczególności ograniczenia celu.

8.9. **Dokumentacja i zgodność**

a) Podmiot odbierający dane niezwłocznie i w odpowiedni sposób rozpatruje sformułowane przez podmiot przekazujący dane zapytania dotyczące przetwarzania na mocy niniejszych klauzul.

b) Strony będą w stanie wykazać przestrzeganie niniejszych klauzul. W szczególności podmiot odbierający dane przechowuje odpowiednią dokumentację czynności przetwarzania wykonanych w imieniu podmiotu przekazującego dane.

c) Podmiot odbierający dane udostępnia podmiotowi przekazującemu dane wszelkie informacje niezbędne, aby wykazać przestrzeganie obowiązków określonych w niniejszych klauzulach oraz aby na żądanie podmiotu przekazującego dane umożliwić przeprowadzenie audytów czynności przetwarzania objętych niniejszymi klauzulami w rozsądnych odstępach czasu lub w przypadku wystąpienia oznak niespełnienia tych obowiązków, a także aby wnieść wkład w te audyty. Podejmując decyzję dotyczącą przeprowadzenia przeglądu lub audytu podmiot przekazujący dane może uwzględnić certyfikacje posiadane przez podmiot odbierający dane.

d) Podmiot przekazujący dane może przeprowadzić audyt samodzielnie lub zlecić jego przeprowadzenie niezależnemu audytorowi. Audyty mogą obejmować kontrole w siedzibie lub obiektach podmiotu odbierającego dane i, w stosownych przypadkach, przeprowadzane są po powiadomieniu z rozsądnym wyprzedzeniem.

e) Strony udostępniają właściwym organom nadzorczym na żądanie informacje, o których mowa w lit. b) i c), w tym wyniki wszelkich audytów.

([4]) W Porozumieniu o Europejskim Obszarze Gospodarczym (Porozumienie EOG) przewidziano rozszerzenie rynku wewnętrznego Unii Europejskiej na trzy państwa EOG – Islandię, Liechtenstein i Norwegię. Unijne prawodawstwo dotyczące ochrony danych, w tym rozporządzenie (UE) 2016/679, jest objęte Porozumieniem EOG i zostało włączone do jego załącznika XI. W związku z tym wszelkie ujawnianie danych stronie trzeciej zlokalizowanej w EOG przez podmiot odbierający dane nie kwalifikuje się jako dalsze przekazanie do celów niniejszych klauzul.

MODUŁ TRZECI: Przekazywanie między podmiotami przetwarzającymi

8.1. **Polecenie**

a) Podmiot przekazujący dane poinformował podmiot odbierający dane, że działa jako podmiot przetwarzający na polecenie administratora/administratorów danych, które to polecenie podmiot przekazujący dane udostępnia podmiotowi odbierającemu dane przed ich przetwarzaniem.

b) Podmiot odbierający dane przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora, zakomunikowane podmiotowi odbierającemu dane przez podmiot przekazujący dane, oraz na każde dodatkowe udokumentowane polecenia podmiotu przekazującego dane. Takie dodatkowe polecenia nie mogą być sprzeczne z poleceniami administratora. Administrator lub podmiot przekazujący dane może wydawać dalsze udokumentowane polecenia dotyczące przetwarzania danych w okresie obowiązywania umowy.

c) Podmiot odbierający dane niezwłocznie informuje podmiot przekazujący dane, jeżeli nie może wykonać tego polecenia. Jeżeli podmiot odbierający dane nie może wykonać polecenia administratora, podmiot przekazujący dane niezwłocznie zgłasza ten fakt administratorowi.

d) Podmiot przekazujący gwarantuje, że na podmiot odbierający dane nałożył takie same obowiązki ochrony danych – na mocy prawa Unii lub prawa państwa członkowskiego – jak w umowie lub innym akcie prawnym między administratorem a podmiotem przekazującym dane ([5]).

8.2. **Ograniczenie celu**

Podmiot odbierający dane przetwarza dane osobowe wyłącznie w określonym celu/określonych celach przekazywania, jak wskazano w załączniku I część B, chyba że działa na podstawie dalszych poleceń administratora wydanych podmiotowi odbierającemu dane przez podmiot przekazujący dane lub dalszych poleceń podmiotu przekazującego dane.

8.3. **Przejrzystość**

Podmiot przekazujący dane udostępnia bezpłatnie na żądanie osobie, której dane dotyczą, kopię niniejszych klauzul, w tym dodatku wypełnionego przez Strony. W zakresie koniecznym w celu ochrony tajemnic handlowych lub innych informacji poufnych, w tym danych osobowych, podmiot przekazujący dane może częściowo zredagować tekst dodatku przed udostępnieniem jego kopii, lecz przekazuje stosowne streszczenie, jeżeli bez takiego streszczenia osoba, której dane dotyczą, nie byłaby w stanie zrozumieć treści takiego tekstu lub korzystać ze swoich praw. Na żądanie Strony przekazują osobie, której dane dotyczą, powody zredagowania tekstu, w miarę możliwości bez ujawniania utajnionych informacji.

8.4. **Prawidłowość**

Jeżeli podmiot odbierający dane zda sobie sprawę, że otrzymane przez niego dane osobowe są nieprawidłowe lub nieaktualne, powiadamia o tym bez zbędnej zwłoki podmiot przekazujący dane. W takim przypadku podmiot odbierający dane współpracuje z podmiotem przekazującym dane w celu ich sprostowania lub usunięcia.

8.5. **Czas trwania przetwarzania oraz usuwanie lub zwrot danych**

Przetwarzanie danych przez podmiot odbierający dane odbywa się wyłącznie przez czas określony w załączniku I część B. Po zakończeniu świadczenia usług przetwarzania podmiot odbierający dane, zgodnie z wyborem podmiotu przekazującego dane, albo usuwa wszystkie dane osobowe przetworzone w imieniu administratora i potwierdza podmiotowi przekazującemu dane ich usunięcie, albo zwraca podmiotowi przekazującemu dane wszystkie dane osobowe przetworzone w jego imieniu i usuwa istniejące kopie. Do czasu usunięcia lub zwrotu danych podmiot odbierający dane nadal zapewnia zgodność z niniejszymi klauzulami. Jeżeli lokalne prawo obowiązujące podmiot odbierający dane zabrania zwrotu lub usunięcia danych osobowych, podmiot odbierający dane gwarantuje, że będzie w dalszym ciągu zapewniał przestrzeganie niniejszych klauzul oraz że będzie przetwarzał je wyłącznie w zakresie i w czasie wymaganym przez to prawo lokalne. Zasada ta pozostaje bez uszczerbku dla klauzuli 14, w szczególności wymogu określonego w klauzuli 14 lit. e), aby podmiot odbierający dane zgłaszał w okresie obowiązywania umowy podmiotowi przekazującemu dane, jeżeli ma powody, aby sądzić, że podlega lub zaczął podlegać przepisom lub praktykom niezgodnym z wymogami określonymi w klauzuli 14 lit. a).

([5]) Zob. art. 28 ust. 4 rozporządzenia (UE) 2016/679, a w przypadku gdy administrator jest instytucją lub organem Unii – art. 29 ust. 4 rozporządzenia (UE) 2018/1725.

8.6. **Bezpieczeństwo przetwarzania**

a) Podmiot odbierający dane, a podczas przesyłania również podmiot przekazujący dane, wdraża odpowiednie środki techniczne i organizacyjne w celu zapewnienia bezpieczeństwa danych, w tym ochrony przeciwko naruszeniu bezpieczeństwa prowadzącego do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do tych danych (zwanego dalej „naruszeniem ochrony danych osobowych"). Przy ocenie odpowiedniego poziomu bezpieczeństwa podmioty te uwzględniają stan wiedzy technicznej, koszty wdrażania oraz charakter, zakres, kontekst i cel lub cele przetwarzania, a także ryzyko wynikające z przetwarzania dla osoby, której dane dotyczą. Strony rozważą w szczególności posłużenie się szyfrowaniem lub pseudonimizacją, w tym podczas przesyłania, w przypadkach, gdy cel przetwarzania może być spełniony w ten sposób. W przypadku pseudonimizacji dodatkowe informacje do celu przypisania danych osobowych konkretnej osobie, której dane dotyczą, pozostają, jeżeli jest to możliwe, pod wyłączną kontrolą podmiotu przekazującego dane lub administratora. W ramach obowiązków w trybie niniejszej litery podmiot odbierający dane wdraża co najmniej środki techniczne i organizacyjne określone w załączniku II. Podmiot odbierający dane przeprowadza regularne kontrole, aby zagwarantować, że środki te wciąż zapewniają odpowiedni poziom bezpieczeństwa.

b) Podmiot odbierający dane udziela dostępu do danych członkom swojego personelu wyłącznie w zakresie ściśle niezbędnym do wykonania umowy, zarządzania umową oraz jej monitorowania. Zapewnia on, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania poufności lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania poufności.

c) W przypadku naruszenia ochrony danych osobowych dotyczącego danych osobowych przetwarzanych przez podmiot odbierający dane na podstawie niniejszych klauzul podmiot odbierający dane stosuje odpowiednie środki w celu zaradzenia temu naruszeniu, w tym środki w celu zminimalizowania jego negatywnych skutków. Po stwierdzeniu naruszenia podmiot odbierający dane zgłasza je również bez zbędnej zwłoki podmiotowi przekazującemu dane oraz – w razie potrzeby i w miarę możliwości – administratorowi. Zgłoszenie takie zawiera szczegóły dotyczące punktu kontaktowego, w którym można uzyskać więcej informacji, opis charakteru naruszenia (w tym w miarę możliwości kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie), jego możliwe konsekwencje oraz środki zastosowane lub proponowane w celu zaradzenia naruszeniu ochrony danych, w tym środki w celu zminimalizowania jego ewentualnych negatywnych skutków. Jeżeli oraz w zakresie, w jakim niemożliwe jest udzielenie wszystkich informacji w tym samym czasie, pierwotne zgłoszenie zawiera informacje dostępne w danym momencie, a dalszych informacji udziela się sukcesywnie, bez zbędnej zwłoki w miarę, jak staną się one dostępne.

d) Podmiot odbierający dane współpracuje z podmiotem przekazującym dane i pomaga mu, aby umożliwić podmiotowi przekazującemu dane wypełnienie obowiązków określonych w rozporządzeniu (UE) 2016/679, w szczególności obowiązku powiadomienia administratora, aby ten mógł z kolei powiadomić właściwy organ nadzorczy i poszkodowane osoby, których dane dotyczą, uwzględniając charakter przetwarzania oraz informacje, do których podmiot odbierający dane ma dostęp.

8.7. **Dane wrażliwe**

Gdy przekazywanie obejmuje dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne lub dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej tej osoby lub dane dotyczące wyroków skazujących i czynów zabronionych (zwane dalej „danymi wrażliwymi"), podmiot odbierający dane stosuje szczególne ograniczenia lub dodatkowe zabezpieczenia określone w załączniku I część B.

8.8. **Dalsze przekazywanie danych**

Podmiot odbierający dane ujawnia dane osobowe stronie trzeciej wyłącznie na podstawie udokumentowanego polecenia administratora przekazanego podmiotowi odbierającemu dane przez podmiot przekazujący dane. Ponadto dane mogą zostać ujawnione stronie trzeciej zlokalizowanej poza terytorium Unii Europejskiej ([6]) (w tym samym państwie co podmiot odbierający dane lub w innym państwie trzecim; dalej „dalsze przekazanie") wyłącznie wówczas, gdy strona trzecia jest związana niniejszymi klauzulami bądź zgadza się im podlegać na mocy odpowiedniego modułu lub jeżeli:

(i) dalsze przekazanie odbywa się do państwa objętego decyzją stwierdzającą odpowiedni stopień ochrony, zgodnie z art. 45 rozporządzenia (UE) 2016/679, obejmującą dalsze przekazywanie;

([6]) W Porozumieniu o Europejskim Obszarze Gospodarczym (Porozumienie EOG) przewidziano rozszerzenie rynku wewnętrznego Unii Europejskiej na trzy państwa EOG – Islandię, Liechtenstein i Norwegię. Unijne prawodawstwo dotyczące ochrony danych, w tym rozporządzenie (UE) 2016/679, jest objęte Porozumieniem EOG i zostało włączone do jego załącznika XI. W związku z tym wszelkie ujawnianie danych stronie trzeciej zlokalizowanej w EOG przez podmiot odbierający dane nie kwalifikuje się jako dalsze przekazanie do celów niniejszych klauzul.

(ii) strona trzecia w inny sposób zapewnia odpowiednie zabezpieczenia zgodnie z art. 46 lub 47 rozporządzenia (UE) 2016/679;

(iii) dalsze przekazanie jest niezbędne do ustalenia, dochodzenia lub ochrony roszczeń w kontekście szczególnego postępowania administracyjnego, regulacyjnego lub sądowego; lub

(iv) dalsze przekazanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej.

Wszelkie dalsze przekazanie odbywa się pod warunkiem przestrzegania przez podmiot odbierający dane wszystkich pozostałych zabezpieczeń na mocy niniejszych klauzul, w szczególności ograniczenia celu.

8.9. **Dokumentacja i zgodność**

a) Podmiot odbierający dane niezwłocznie i w odpowiedni sposób rozpatruje zapytania podmiotu przekazującego dane lub administratora dotyczące przetwarzania na mocy niniejszych klauzul.

b) Strony będą w stanie wykazać przestrzeganie niniejszych klauzul. W szczególności podmiot odbierający dane przechowuje odpowiednią dokumentację czynności przetwarzania wykonanych w imieniu administratora.

c) Podmiot odbierający dane udostępnia podmiotowi przekazującemu dane wszelkie informacje niezbędne, aby wykazać przestrzeganie obowiązków określonych w niniejszych klauzulach, a podmiot przekazujący dane przekazuje te informacje administratorowi.

d) Podmiot odbierający dane umożliwia przeprowadzanie przez podmiot przekazujący dane audytów czynności przetwarzania objętych niniejszymi klauzulami w rozsądnych odstępach czasu lub w przypadku wystąpienia oznak niespełnienia tych obowiązków, a także wnosi wkład w te audyty. Dotyczy to również sytuacji, w których podmiot przekazujący dane żąda audytu wykonania polecenia administratora. Podejmując decyzję dotyczącą przeprowadzenia audytu, podmiot przekazujący dane może uwzględnić odpowiednie certyfikacje posiadane przez podmiot odbierający dane.

e) Jeżeli audyt dotyczy polecenia administratora, podmiot przekazujący dane udostępnia wyniki administratorowi.

f) Podmiot przekazujący dane może przeprowadzić audyt samodzielnie lub zlecić jego przeprowadzenie niezależnemu audytorowi. Audyty mogą obejmować kontrole w siedzibie lub obiektach podmiotu odbierającego dane i, w stosownych przypadkach, przeprowadzane są po powiadomieniu z rozsądnym wyprzedzeniem.

g) Strony udostępniają właściwym organom nadzorczym na żądanie informacje, o których mowa w lit. b) i c), w tym wyniki wszelkich audytów.

MODUŁ CZWARTY: Przekazywanie przez podmiot przetwarzający administratorowi

8.1. **Polecenie**

a) Podmiot przekazujący dane przetwarza dane osobowe wyłącznie na udokumentowane polecenie podmiotu odbierającego dane występującego w roli administratora.

b) Podmiot przekazujący dane niezwłocznie powiadamia podmiot odbierający dane, jeżeli nie może wykonać tego polecenia, w tym jeżeli takie polecenie narusza przepisy rozporządzenia (UE) 2016/679 lub inne przepisy prawa Unii lub państwa członkowskiego dotyczące ochrony danych.

c) Podmiot odbierający dane powinien zaniechać wszelkich działań, które uniemożliwiłyby podmiotowi przekazującemu dane wywiązanie się z obowiązków ciążących na nim na podstawie rozporządzenia (UE) 2016/679, w tym w kontekście podwykonawstwa przetwarzania lub w odniesieniu do współpracy z właściwymi organami nadzorczymi.

d) Po zakończeniu świadczenia usług przetwarzania podmiot przekazujący dane, zgodnie z wyborem podmiotu odbierającego dane, albo usuwa wszystkie dane osobowe przetworzone w imieniu podmiotu odbierającego dane i potwierdza podmiotowi odbierającemu dane ich usunięcie, albo zwraca podmiotowi odbierającemu dane wszystkie dane osobowe przetworzone w jego imieniu i usuwa istniejące kopie.

8.2. **Bezpieczeństwo przetwarzania**

a) Strony wdrażają odpowiednie środki techniczne i organizacyjne w celu zapewnienia bezpieczeństwa danych, w tym podczas przesyłania, oraz ochrony przeciwko naruszeniu bezpieczeństwa prowadzącego do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu (zwanego dalej „naruszeniem ochrony danych osobowych"). Przy ocenie odpowiedniego poziomu bezpieczeństwa podmioty te uwzględniają stan wiedzy technicznej, koszty wdrażania oraz charakter danych osobowych ([7]), charakter, zakres, kontekst i cel lub cele przetwarzania, a także ryzyko wynikające z przetwarzania dla osoby, której dane dotyczą, a w szczególności rozważają posłużenie się szyfrowaniem lub pseudonimizacją, w tym podczas przesyłania, w przypadkach gdy cel przetwarzania może być spełniony w ten sposób.

b) Podmiot przekazujący dane pomaga podmiotowi odbierającemu dane zapewnić odpowiednie bezpieczeństwo danych zgodnie z lit. a). W przypadku naruszenia ochrony danych osobowych dotyczącego danych osobowych przetwarzanych przez podmiot przekazujący dane na mocy niniejszych klauzul podmiot przekazujący dane niezwłocznie powiadamia podmiot odbierający dane, kiedy tylko dowie się, że doszło do takiego naruszenia, i pomaga podmiotowi przekazującemu dane w zaradzeniu temu naruszeniu.

c) Podmiot przekazujący dane zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania poufności lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania poufności.

8.3. **Dokumentacja i zgodność**

a) Strony będą w stanie wykazać przestrzeganie niniejszych klauzul.

b) Podmiot przekazujący dane udostępnia podmiotowi odbierającemu dane wszelkie informacje niezbędne do wykazania przestrzegania obowiązków określonych w niniejszych klauzulach oraz do umożliwienia przeprowadzania audytów, a także wniesienia wkładu w te audyty.

Klauzula 9

Korzystanie z usług podwykonawców przetwarzania

MODUŁ DRUGI: Przekazywanie przez administratora podmiotowi przetwarzającemu

a) WARIANT 1: UPRZEDNIA SZCZEGÓŁOWA ZGODA Podmiot odbierający dane nie może zlecać w ramach podwykonawstwa żadnych czynności przetwarzania realizowanych w imieniu podmiotu przekazującego dane na podstawie niniejszych klauzul podwykonawcy przetwarzania bez uzyskania uprzedniej szczegółowej pisemnej zgody podmiotu przekazującego dane. Podmiot odbierający dane przedstawia wniosek o udzielenie szczegółowej zgody przynajmniej [*należy wskazać termin*] przed zaangażowaniem podwykonawcy przetwarzania, wraz z informacjami, których podmiot przekazujący dane potrzebuje do podjęcia decyzji w sprawie wydania zgody. Załącznik III zawiera wykaz podwykonawców przetwarzania już upoważnionych przez podmiot przekazujący dane. Strony są obowiązane do aktualizacji załącznika III.

WARIANT 2: OGÓLNA PISEMNA ZGODA Podmiot odbierający dane ma ogólną zgodę podmiotu przekazującego dane na angażowanie podwykonawców przetwarzania widniejących w uzgodnionym wykazie. Podmiot odbierający dane wyraźnie informuje na piśmie podmiot przekazujący dane o wszelkich zamierzonych zmianach w tym wykazie polegających na dodaniu lub zastąpieniu podwykonawców przetwarzania z wyprzedzeniem wynoszącym co najmniej [*określić przedział czasu*], dając w ten sposób podmiotowi przekazującemu dane wystarczający czas na wyrażenie sprzeciwu wobec takich zmian przed zaangażowaniem podwykonawcy lub podwykonawców przetwarzania. Podmiot odbierający dane dostarcza podmiotowi przekazującemu dane informacje niezbędne do umożliwienia mu wykonania prawa do sprzeciwu.

b) Jeżeli podmiot odbierający dane angażuje podwykonawcę przetwarzania do celów wykonania określonych czynności przetwarzania (w imieniu podmiotu przekazującego dane), czyni to na podstawie pisemnej umowy, która zasadniczo przewiduje takie same obowiązki w odniesieniu do ochrony danych, jakie wiążą podmiot odbierający dane na mocy niniejszych klauzul, w tym w zakresie praw osób, których dane dotyczą, przysługujących im jako osobom trzecim, na rzecz których zawarto umowę ([8]). Strony uzgadniają, że przestrzegając niniejszej klauzuli, podmiot odbierający dane wypełnia swoje obowiązki wynikające z klauzuli 8.8. Podmiot odbierający dane zapewnia, aby podwykonawca przetwarzania wywiązywał się z obowiązków, którym podmiot odbierający dane podlega na podstawie niniejszych klauzul.

([7]) Obejmuje to kwestię, czy przekazywanie i dalsze przetwarzanie dotyczy danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne lub dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej tej osoby lub dane dotyczące wyroków skazujących lub czynów zabronionych.

([8]) Podwykonawca przetwarzania może spełnić ten wymóg, przystępując do niniejszych klauzul na podstawie odpowiedniego modułu zgodnie z klauzulą 7.

c) Na żądanie podmiotu przekazującego dane podmiot odbierający dane przekazuje podmiotowi przekazującemu dane kopię umowy dotyczącej podwykonawstwa przetwarzania oraz wszelkich późniejszych zmian. W zakresie koniecznym do zapewnienia ochrony tajemnic handlowych lub innych informacji poufnych, w tym danych osobowych, podmiot odbierający dane może zredagować tekst umowy przed udostępnieniem jej kopii.

d) Podmiot odbierający dane pozostaje w pełni odpowiedzialny wobec podmiotu przekazującego dane za wykonywanie obowiązków podwykonawcy przetwarzania wynikających z umowy zawartej przez niego z podmiotem odbierającym dane. Podmiot odbierający dane powiadamia podmiot przekazujący dane o każdym przypadku niewypełnienia przez podwykonawcę przetwarzania obowiązków wynikających z tej umowy.

e) Podmiot odbierający dane uzgadnia z podwykonawcą przetwarzania klauzulę na rzecz osoby trzeciej, na rzecz której zawarto umowę, na mocy której to klauzuli – w przypadku gdy podmiot odbierający dane przestał istnieć faktycznie lub formalnie lub stał się niewypłacalny – podmiot przekazujący dane ma prawo rozwiązać umowę dotyczącą podwykonawstwa przetwarzania i polecić podwykonawcy przetwarzania usunięcie lub zwrot danych osobowych.

MODUŁ TRZECI: Przekazywanie między podmiotami przetwarzającymi

a) WARIANT 1: UPRZEDNIA SZCZEGÓŁOWA ZGODA Podmiot odbierający dane nie może zlecać w ramach podwykonawstwa żadnych czynności przetwarzania realizowanych w imieniu podmiotu przekazującego dane na podstawie niniejszych klauzul podwykonawcy przetwarzania bez uzyskania uprzedniej szczegółowej pisemnej zgody administratora. Podmiot odbierający dane przedstawia wniosek o udzielenie szczegółowej zgody przynajmniej [*należy wskazać termin*] przed zaangażowaniem podwykonawcy przetwarzania, wraz z informacjami, których administrator potrzebuje do podjęcia decyzji w sprawie wydania zgody. Podmiot ten informuje o takim zaangażowaniu podmiot przekazujący dane. Załącznik III zawiera wykaz podwykonawców przetwarzania już upoważnionych przez administratora. Strony są obowiązane do aktualizacji załącznika III.

WARIANT 2: OGÓLNA PISEMNA ZGODA Podmiot odbierający dane ma ogólną zgodę administratora na angażowanie podwykonawców przetwarzania widniejących w uzgodnionym wykazie. Podmiot odbierający dane wyraźnie informuje administratora na piśmie o wszelkich zamierzonych zmianach w tym wykazie polegających na dodaniu lub zastąpieniu podwykonawców przetwarzania z wyprzedzeniem wynoszącym co najmniej [*określić przedział czasu*], dając w ten sposób administratorowi wystarczający czas na wyrażenie sprzeciwu wobec takich zmian przed zaangażowaniem podwykonawcy lub podwykonawców przetwarzania. Podmiot odbierający dane dostarcza administratorowi informacje niezbędne do umożliwienia mu wykonania prawa do sprzeciwu. Podmiot odbierający dane informuje podmiot przekazujący dane o zaangażowaniu podwykonawcy lub podwykonawców przetwarzania.

b) Jeżeli podmiot odbierający dane angażuje podwykonawcę przetwarzania do celów wykonania określonych czynności przetwarzania (w imieniu administratora), czyni to na podstawie pisemnej umowy, która zasadniczo przewiduje takie same obowiązki w odniesieniu do ochrony danych, jakie wiążą podmiot odbierający dane na mocy niniejszych klauzul, w tym w zakresie praw osób, których dane dotyczą, przysługujących im jako osobom trzecim, na rzecz których zawarto umowę (9). Strony uzgadniają, że przestrzegając niniejszej klauzuli, podmiot odbierający dane wypełnia swoje obowiązki wynikające z klauzuli 8.8. Podmiot odbierający dane zapewnia, aby podwykonawca przetwarzania wywiązywał się z obowiązków, którym podmiot odbierający dane podlega na podstawie niniejszych klauzul.

c) Na żądanie podmiotu przekazującego dane lub administratora podmiot odbierający dane przekazuje kopię umowy dotyczącej podwykonawstwa przetwarzania oraz wszelkich późniejszych zmian. W zakresie koniecznym do zapewnienia ochrony tajemnic handlowych lub innych informacji poufnych, w tym danych osobowych, podmiot odbierający dane może zredagować tekst umowy przed udostępnieniem jej kopii.

d) Podmiot odbierający dane pozostaje w pełni odpowiedzialny wobec podmiotu przekazującego dane za wykonywanie obowiązków podwykonawcy przetwarzania wynikających z umowy zawartej przez niego z podmiotem odbierającym dane. Podmiot odbierający dane powiadamia podmiot przekazujący dane o każdym przypadku niewypełnienia przez podwykonawcę przetwarzania obowiązków wynikających z tej umowy.

e) Podmiot odbierający dane uzgadnia z podwykonawcą przetwarzania klauzulę na rzecz osoby trzeciej, na rzecz której zawarto umowę, na mocy której to klauzuli – w przypadku gdy podmiot odbierający dane przestał istnieć faktycznie lub formalnie lub stał się niewypłacalny – podmiot przekazujący dane ma prawo rozwiązać umowę dotyczącą podwykonawstwa przetwarzania i polecić podwykonawcy przetwarzania usunięcie lub zwrot danych osobowych.

(9) Podwykonawca przetwarzania może spełnić ten wymóg, przystępując do niniejszych klauzul na podstawie odpowiedniego modułu zgodnie z klauzulą 7.

Klauzula 10

Prawa osoby, której dane dotyczą

MODUŁ PIERWSZY: Przekazywanie między administratorami

a) Podmiot odbierający dane, w stosownych przypadkach z pomocą podmiotu przekazującego dane, rozpatrzy – bez zbędnej zwłoki, a najpóźniej w terminie jednego miesiąca od otrzymania zapytania lub żądania – wszelkie zapytania i żądania otrzymane od osoby, której dane dotyczą, związane z przetwarzaniem jej danych osobowych i wykonywaniem jej praw na mocy niniejszych klauzul ([10]). Podmiot odbierający dane stosuje odpowiednie środki mające na celu ułatwienie występowania z takimi zapytaniami i żądaniami oraz wykonywania praw osób, których dane dotyczą. Wszelkie informacje przekazywane osobie, której dane dotyczą, muszą być podane w zrozumiałej i łatwo dostępnej formie, przy użyciu jasnego i prostego języka.

b) W szczególności, na żądanie osoby, której dane dotyczą, podmiot odbierający dane jest zobowiązany do nieodpłatnego:

   (i) przekazania osobie, której dane dotyczą, potwierdzenia, czy dotyczące jej dane osobowe są przetwarzane – a jeżeli przetwarzanie takie ma miejsce – kopii odnoszących się do niej danych oraz informacji określonych w załączniku I; jeżeli dane osobowe zostały lub zostaną dalej przekazane – przekazania informacji o odbiorcach lub kategoriach odbiorców (w stosownych przypadkach w celu dostarczenia istotnych informacji), którym dane osobowe zostały lub zostaną dalej przekazane, o celu takiego dalszego przekazywania i jego podstawie wynikającej z klauzuli 8.7 oraz przekazania informacji o prawie do wniesienia skargi do organu nadzorczego zgodnie z klauzulą 12 lit. c) ppkt (i);

   (ii) sprostowania nieprawidłowych lub uzupełnienia niekompletnych danych odnoszących się do osoby, której dane dotyczą;

   (iii) usunięcia danych osobowych osoby, której dane dotyczą, jeżeli dane te są lub były przetwarzane z naruszeniem którejkolwiek z niniejszych klauzul zapewniających przysługiwanie jej praw jako osobie trzeciej, na rzecz której zawarto umowę, lub jeżeli osoba, której dane dotyczą, wycofa zgodę, na podstawie której przetwarzanie się odbywa.

c) Jeżeli podmiot odbierający dane przetwarza dane osobowe do celów marketingu bezpośredniego, musi zaprzestać takiego przetwarzania, jeżeli osoba, której dane dotyczą, wniesie sprzeciw wobec takiego przetwarzania.

d) Podmiot odbierający dane nie może podjąć decyzji opierającej się jedynie na zautomatyzowanym przetwarzaniu przekazanych danych osobowych (zwanym dalej „zautomatyzowanym podejmowaniem decyzji"), która to decyzja wywoływałaby skutki prawne względem osoby, której dane dotyczą, lub wywierałaby na nią podobny znaczący wpływ, o ile taki podmiot nie uzyskał wyraźnej zgody osoby, której dane dotyczą, lub nie został do tego upoważniony na mocy przepisów państwa przeznaczenia, o ile przepisy te obejmują stosowne środki w celu zabezpieczenia praw i uzasadnionych interesów osoby, której dane dotyczą. W takim przypadku podmiot odbierający dane, w razie potrzeby we współpracy z podmiotem przekazującym dane, musi:

   (i) poinformować osobę, której dane dotyczą, o planowanym zautomatyzowanym podejmowaniu decyzji, przewidywanych konsekwencjach oraz o zasadach podejmowania decyzji oraz

   (ii) wdrożyć odpowiednie zabezpieczenia, przynajmniej poprzez umożliwienie osobie, której dane dotyczą, zakwestionowania decyzji, wyrażenia swojego punktu widzenia i zyskania możliwości przeprowadzenia weryfikacji przez człowieka.

e) Jeżeli żądania osoby, której dane dotyczą, są nadmierne, w szczególności ze względu na swój ustawiczny charakter, podmiot odbierający dane może pobrać rozsądną opłatę, uwzględniając administracyjne koszty spełnienia żądania, albo odmówić podjęcia działań w związku z żądaniem.

f) Podmiot odbierający dane może odmówić spełnienia żądania osoby, której dane dotyczą, jeżeli taka odmowa jest dozwolona na mocy przepisów państwa przeznaczenia oraz w demokratycznym społeczeństwie jest środkiem niezbędnym i proporcjonalnym służącym ochronie jednego z celów wymienionych w art. 23 ust. 1 rozporządzenia (UE) 2016/679.

g) W przypadku gdy podmiot odbierający dane zamierza odmówić spełnienia żądania osoby, której dane dotyczą, informuje ją o przyczynach odmowy oraz o możliwości złożenia skargi do właściwego organu nadzorczego lub dochodzenia roszczeń na drodze sądowej.

MODUŁ DRUGI: Przekazywanie przez administratora podmiotowi przetwarzającemu

a) Podmiot odbierający dane bezzwłocznie powiadamia podmiot przekazujący dane o każdym żądaniu otrzymanym od osoby, której dane dotyczą. Nie odpowiada on na to żądanie samodzielnie, chyba że został do tego upoważniony przez podmiot przekazujący dane.

([10]) Termin ten można przedłużyć w niezbędnym zakresie maksymalnie o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań. Podmiot odbierający dane należycie i niezwłocznie informuje osobę, której dane dotyczą, o każdym takim przedłużeniu.

b) Podmiot odbierający dane pomaga podmiotowi przekazującemu dane w wypełnianiu jego obowiązków w zakresie odpowiadania na żądania osób, których dane dotyczą, związane z wykonywaniem praw przysługujących tym osobom na podstawie rozporządzenia (UE) 2016/679. W związku z tym Strony określają w załączniku II odpowiednie środki techniczne i organizacyjne, uwzględniając charakter przetwarzania, w drodze których zapewniana będzie pomoc, jak również zakres wymaganej pomocy.

c) Wywiązując się z obowiązków spoczywających na nim na podstawie lit. a) i b), podmiot odbierający dane postępuje zgodnie z poleceniem podmiotu przekazującego dane.

MODUŁ TRZECI: Przekazywanie między podmiotami przetwarzającymi

a) Podmiot odbierający dane bezzwłocznie powiadamia podmiot przekazujący dane i – w stosownych przypadkach – administratora o każdym żądaniu otrzymanym od osoby, której dane dotyczą, i nie odpowiada na to żądanie, chyba że został do tego upoważniony przez administratora.

b) Podmiot odbierający dane pomaga administratorowi, w razie potrzeby we współpracy z podmiotem przekazującym dane, w wypełnianiu jego obowiązków w zakresie odpowiadania na żądania osób, których dane dotyczą, związane z wykonywaniem praw przysługujących tym osobom na podstawie rozporządzenia (UE) 2016/679 lub w stosownych przypadkach rozporządzenia (UE) 2018/1725. W związku z tym Strony określają w załączniku II odpowiednie środki techniczne i organizacyjne, uwzględniając charakter przetwarzania, w drodze których zapewniana będzie pomoc, jak również zakres wymaganej pomocy.

c) Wywiązując się z obowiązków spoczywających na nim na podstawie lit. a) i b), podmiot odbierający dane postępuje zgodnie z poleceniem administratora przekazanym przez podmiot przekazujący dane.

MODUŁ CZWARTY: Przekazywanie przez podmiot przetwarzający administratorowi

Strony udzielają sobie wzajemnej pomocy w zakresie zapytań i żądań ze strony osób, których dane dotyczą, zgodnie z lokalnym prawem, któremu podlega podmiot odbierający dane, lub – w przypadku przetwarzania danych w Unii przez podmiot przekazujący dane – zgodnie z rozporządzeniem (UE) 2016/679.

Klauzula 11

Dochodzenie roszczeń

a) Podmiot odbierający dane – w sposób przejrzysty i łatwo dostępny w drodze indywidualnego zawiadomienia lub na swojej stronie internetowej – informuje osoby, których dane dotyczą, o tym, który punkt kontaktowy jest upoważniony do rozpatrywania skarg. Podmiot ten niezwłocznie rozpatruje wszelkie skargi otrzymane od osoby, której dane dotyczą.

[WARIANT: Podmiot odbierający dane wyraża zgodę, aby osoby, których dane dotyczą, mogły złożyć skargę również do niezależnego organu rozstrzygania sporów ([11]) bez obciążania kosztami osoby, której dane dotyczą. W sposób określony w lit. a) informuje on osoby, których dane dotyczą, o takim mechanizmie dochodzenia roszczeń oraz o tym, że nie mają one obowiązku korzystać z niego ani postępować zgodnie z konkretną procedurą podczas dochodzenia roszczeń.]

MODUŁ PIERWSZY: Przekazywanie między administratorami

MODUŁ DRUGI: Przekazywanie przez administratora podmiotowi przetwarzającemu

MODUŁ TRZECI: Przekazywanie między podmiotami przetwarzającymi

b) W przypadku gdy między osobą, której dane dotyczą, a jedną ze Stron wystąpi spór co do przestrzegania klauzul, Strona ta dokłada wszelkich starań, aby rozwiązać spór w sposób polubowny i terminowy. Strony na bieżąco przekazują sobie informacje na temat pojawienia się takich sporów i w stosownych przypadkach współpracują, by je rozwiązać.

c) W przypadku gdy osoba, której dane dotyczą, powoła się na wynikające z klauzuli 3 prawo przysługujące jej jako osobie trzeciej, na rzecz której zawarto umowę, podmiot odbierający dane akceptuje decyzję osoby, której dane dotyczą, aby:

(i) złożyć skargę do organu nadzorczego w państwie członkowskim miejsca zwykłego pobytu lub miejsca pracy tej osoby lub do właściwego organu nadzorczego zgodnie z klauzulą 13;

(ii) skierować spór do sądów właściwych w rozumieniu klauzuli 18.

([11]) Podmiot odbierający dane może zaoferować możliwość niezależnego rozwiązywania sporów za pośrednictwem sądu arbitrażowego wyłącznie wówczas, gdy posiada jednostkę organizacyjną w państwie, które ratyfikowało Konwencję nowojorską o uznawaniu i wykonywaniu zagranicznych orzeczeń arbitrażowych.

d) Strony akceptują, że osobę, której dane dotyczą, mogą reprezentować podmiot, organizacja lub zrzeszenie, które nie mają charakteru zarobkowego, na warunkach określonych w art. 80 ust. 1 rozporządzenia (UE) 2016/679.

e) Podmiot odbierający dane stosuje się do decyzji wiążącej na podstawie obowiązującego prawa Unii lub państwa członkowskiego.

f) Podmiot odbierający dane potwierdza, że wybór, jakiego dokona osoba, której dane dotyczą, pozostanie bez uszczerbku dla praw podmiotowych lub procesowych przysługujących jej zgodnie z mającymi zastosowanie przepisami.

Klauzula 12

Odpowiedzialność

MODUŁ PIERWSZY: Przekazywanie między administratorami

MODUŁ CZWARTY: Przekazywanie przez podmiot przetwarzający administratorowi

a) Każda Strona ponosi odpowiedzialność wobec podmiotu lub podmiotów będących drugą Stroną za wszelkie wyrządzone im przez siebie szkody wynikające z naruszenia niniejszych klauzul.

b) Każda Strona ponosi odpowiedzialność wobec osoby, której dane dotyczą, a osobie, której dane dotyczą, przysługuje prawo do odszkodowania z tytułu jakichkolwiek szkód majątkowych lub niemajątkowych wyrządzonych osobie, której dane dotyczą, przez Stronę w wyniku naruszenia praw przysługujących jej jako osobie trzeciej, na rzecz której zawarto umowę, na podstawie niniejszych klauzul. Zasada ta pozostaje bez uszczerbku dla odpowiedzialności spoczywającej na podmiocie przekazującym dane na podstawie rozporządzenia (UE) 2016/679.

c) W przypadku gdy za jakiekolwiek szkody wobec osoby, której dane dotyczą, wynikające z naruszenia niniejszych klauzul, odpowiedzialność ponosi więcej niż jednak Strona, wszystkie odpowiedzialne Strony ponoszą odpowiedzialność solidarną, a osobie, której dane dotyczą, przysługuje prawo do wystąpienia do sądu przeciwko którejkolwiek z tych Stron.

d) Strony uzgadniają, że w przypadku pociągnięcia na podstawie lit. c) jednej Strony do odpowiedzialności przysługuje jej prawo do żądania od podmiotu lub podmiotów będących drugą Stroną odszkodowania w wysokości odpowiadającej stopniowi odpowiedzialności za wyrządzoną szkodę.

e) Podmiot odbierający dane nie może powołać się na postępowanie podmiotu przetwarzającego ani podwykonawcy przetwarzania, aby uniknąć własnej odpowiedzialności.

MODUŁ DRUGI: Przekazywanie przez administratora podmiotowi przetwarzającemu

MODUŁ TRZECI: Przekazywanie między podmiotami przetwarzającymi

a) Każda Strona ponosi odpowiedzialność wobec podmiotu lub podmiotów będących drugą Stroną za wszelkie wyrządzone im przez siebie szkody wynikające z naruszenia niniejszych klauzul.

b) Podmiot odbierający dane ponosi odpowiedzialność wobec osoby, której dane dotyczą, a osobie, której dane dotyczą, przysługuje prawo do odszkodowania z tytułu jakichkolwiek szkód majątkowych lub niemajątkowych wyrządzonych osobie, której dane dotyczą, przez podmiot odbierający dane lub jego podwykonawcę przetwarzania w wyniku naruszenia praw przysługujących jej jako osobie trzeciej, na rzecz której zawarto umowę, na podstawie niniejszych klauzul.

c) Niezależnie od postanowień lit. b) podmiot przekazujący dane ponosi odpowiedzialność wobec osoby, której dane dotyczą, a osobie, której dane dotyczą, przysługuje prawo do odszkodowania z tytułu jakichkolwiek szkód majątkowych lub niemajątkowych wyrządzonych osobie, której dane dotyczą, przez podmiot przekazujący dane lub podmiot odbierający dane (lub jego podwykonawcę przetwarzania) w wyniku naruszenia praw przysługujących jej jako osobie trzeciej, na rzecz której zawarto umowę, na podstawie niniejszych klauzul. Zasada ta pozostaje bez uszczerbku dla odpowiedzialności spoczywającej na podmiocie przekazującym dane, a w przypadku gdy podmiot przekazujący dane jest podmiotem przetwarzającym działającym w imieniu administratora – bez uszczerbku dla odpowiedzialności administratora na podstawie rozporządzenia (UE) 2016/679 lub w stosownych przypadkach rozporządzenia (UE) 2018/1725.

d) Strony uzgadniają, że w przypadku pociągnięcia na podstawie postanowień lit. c) podmiotu przekazującego dane do odpowiedzialności za szkody wyrządzone przez podmiot odbierający dane (lub jego podwykonawcę przetwarzania) przysługuje mu prawo do żądania od podmiotu odbierającego dane odszkodowania w wysokości odpowiadającej stopniowi odpowiedzialności podmiotu odbierającego dane za wyrządzoną szkodę.

e) W przypadku gdy za jakiekolwiek szkody wobec osoby, której dane dotyczą, wynikające z naruszenia niniejszych klauzul, odpowiedzialność ponosi więcej niż jednak Strona, wszystkie odpowiedzialne Strony ponoszą odpowiedzialność solidarną, a osobie, której dane dotyczą, przysługuje prawo do wystąpienia do sądu przeciwko którejkolwiek z tych Stron.

f) Strony uzgadniają, że w przypadku pociągnięcia na podstawie postanowień lit. e) jednej Strony do odpowiedzialności przysługuje jej prawo do żądania od podmiotu lub podmiotów będących drugą Stroną odszkodowania w wysokości odpowiadającej stopniowi odpowiedzialności za wyrządzoną szkodę.

g) Podmiot odbierający dane nie może powołać się na postępowanie podwykonawcy przetwarzania, aby uniknąć własnej odpowiedzialności.

Klauzula 13

Nadzór

MODUŁ PIERWSZY: Przekazywanie między administratorami

MODUŁ DRUGI: Przekazywanie przez administratora podmiotowi przetwarzającemu

MODUŁ TRZECI: Przekazywanie między podmiotami przetwarzającymi

a) [W przypadku gdy podmiot przekazujący dane posiada jednostkę organizacyjną w państwie członkowskim UE:] Organ nadzorczy odpowiedzialny za zapewnianie, aby podmiot przekazujący dane przestrzegał przepisów rozporządzenia (UE) 2016/679 w odniesieniu do przekazywania danych, jak wskazano w załączniku I część C, działa w charakterze właściwego organu nadzorczego.

[W przypadku gdy podmiot przekazujący dane nie ma jednostki organizacyjnej w państwie członkowskim UE, lecz jest objęty terytorialnym zakresem stosowania rozporządzenia (UE) 2016/679 zgodnie z art. 3 ust. 2 tego rozporządzenia i wyznaczył przedstawiciela na podstawie art. 27 ust. 1 rozporządzenia (UE) 2016/679:] Organ nadzorczy państwa członkowskiego, w którym przedstawiciel w rozumieniu art. 27 ust. 1 rozporządzenia (UE) 2016/679 posiada jednostkę organizacyjną, jak wskazano w załączniku I część C, działa w charakterze właściwego organu nadzorczego.

[W przypadku gdy podmiot przekazujący dane nie ma jednostki organizacyjnej w państwie członkowskim UE, lecz jest objęty terytorialnym zakresem stosowania rozporządzenia (UE) 2016/679 zgodnie z art. 3 ust. 2 tego rozporządzenia, jednak nie wyznaczył przedstawiciela na podstawie art. 27 ust. 2 rozporządzenia (UE) 2016/679:] Organ nadzorczy z jednego z państw członkowskich, w którym przebywają osoby, których dane dotyczą, których dane osobowe są przekazywane na podstawie niniejszych klauzul w związku z oferowaniem im towarów lub usług lub których zachowanie jest monitorowane, jak wskazano w załączniku I część C, działa w charakterze właściwego organu nadzorczego.

b) Podmiot odbierający dane zgadza się poddać jurysdykcji właściwego organu nadzorczego i współpracować z tym organem w zakresie wszystkich procedur ukierunkowanych na zapewnienie przestrzegania niniejszych klauzul. W szczególności podmiot odbierający dane zgadza się odpowiadać na zapytania, poddawać się audytom i przestrzegać środków przyjętych przez organ nadzorczy, w tym środków zaradczych i kompensacyjnych. Przedstawia on organowi nadzorczemu pisemne potwierdzenie podjęcia się realizacji niezbędnych działań.

SEKCJA III – LOKALNE PRAWA I OBOWIĄZKI W PRZYPADKU DOSTĘPU PRZEZ ORGANY PUBLICZNE

Klauzula 14

Prawa i praktyki lokalne wpływające na przestrzeganie klauzul

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*(w przypadku gdy podmiot przetwarzający z UE łączy dane osobowe otrzymane od administratora z państwa trzeciego z danymi osobowymi zgromadzonym przez administratora w UE)*

a) Strony gwarantują, że nie mają podstaw, by uważać, iż prawa i praktyki w państwie trzecim przeznaczenia, mające zastosowanie do przetwarzania danych osobowych przez podmiot odbierający dane, w tym wszelkie wymogi dotyczące ujawniania danych osobowych lub środki upoważniające organy publiczne do uzyskania dostępu, uniemożliwiają podmiotowi odbierającemu dane wypełnienie jego obowiązków wynikających z niniejszych klauzul. Opiera się to na założeniu, że przepisy i praktyki, które nie naruszają istoty podstawowych praw i wolności oraz nie wykraczają poza to, co jest w demokratycznym społeczeństwie środkiem niezbędnym i proporcjonalnym służącym zabezpieczeniu jednego z celów wymienionych w art. 23 ust. 1 rozporządzenia (UE) 2016/679, nie są sprzeczne z niniejszymi klauzulami.

b) Strony oświadczają, że składając gwarancję, o której mowa w lit. a), należycie uwzględniły w szczególności następujące elementy:

(i) szczególne okoliczności przekazywania, w tym długość łańcucha przetwarzania, liczbę zaangażowanych podmiotów i wykorzystywane kanały przekazywania; planowane dalsze przekazywanie; rodzaj odbiorcy; cel przetwarzania danych; kategorie i format przekazywanych danych osobowych; sektor gospodarki, w którym dochodzi do przekazywania danych; miejsce przechowywania przekazywanych danych;

(ii) przepisy i praktyki państwa trzeciego przeznaczenia, w tym przepisy i praktyki wymagające ujawnienia danych organom publicznym lub upoważniające takie organy do uzyskania dostępu, istotne w świetle szczególnych okoliczności przekazywania danych oraz mających zastosowanie ograniczeń i zabezpieczeń ([12]);

(iii) wszelkie stosowne zabezpieczenia umowne, techniczne lub organizacyjne wprowadzone w celu uzupełnienia zabezpieczeń wynikających z niniejszych klauzul, w tym środki stosowane w czasie przekazywania i przetwarzania danych osobowych w państwie przeznaczenia.

c) Podmiot odbierający dane gwarantuje, że przeprowadzając ocenę na podstawie postanowień lit. b), dołożył wszelkich starań, aby udostępnić podmiotowi przekazującemu dane odpowiednie informacje, oraz wyraża zgodę na dalszą współpracę z podmiotem przekazującym dane w zakresie zapewnienia zgodności z niniejszymi klauzulami.

d) Strony zgadzają się udokumentować ocenę, o której mowa w lit. b), i udostępnić ją na żądanie właściwego organu nadzorczego.

e) Podmiot odbierający dane zobowiązuje się do niezwłocznego powiadomienia podmiotu przekazującego dane, jeśli po uzgodnieniu niniejszych klauzul i w okresie obowiązywania umowy ma powody, aby sądzić, że podlega lub zaczął podlegać przepisom lub praktykom niezgodnym z wymogami określonymi w lit. a), w tym w wyniku zmiany przepisów państwa trzeciego lub środka (takiego jak żądanie ujawnienia danych) wskazującego na stosowanie takich przepisów w praktyce, które nie jest zgodne z wymogami określonymi w lit. a). [W przypadku modułu trzeciego: Podmiot przekazujący dane przekazuje to powiadomienie administratorowi.]

f) Po otrzymaniu powiadomienia zgodnie z lit. e) lub jeżeli podmiot przekazujący dane ma inny powód, by sądzić, że podmiot odbierający dane nie może dłużej wypełniać swoich obowiązków wynikających z niniejszych klauzul, podmiot przekazujący dane bezzwłocznie określa odpowiednie środki (na przykład środki techniczne lub organizacyjne służące zapewnieniu bezpieczeństwa i poufności), które podmiot przekazujący dane lub podmiot odbierający dane powinni przyjąć w celu zaradzenia zaistniałej sytuacji [w przypadku modułu trzeciego: w stosownych przypadkach w porozumieniu z administratorem]. Podmiot przekazujący dane wstrzymuje przekazywanie danych, jeżeli uzna, że zapewnienie odpowiednich zabezpieczeń w odniesieniu do takiego przekazywania jest niemożliwe, lub na polecenie [w przypadku modułu trzeciego: administratora lub] właściwego organu nadzorczego. W takim przypadku podmiot przekazujący dane jest uprawniony do rozwiązania umowy – o ile problem dotyczy przetwarzania danych osobowych na podstawie niniejszych klauzul. W przypadku gdy umowa dotyczy więcej niż dwóch Stron, podmiot przekazujący dane może skorzystać z tego prawa do rozwiązania umowy tylko w odniesieniu do odpowiedniej Strony, chyba że Strony uzgodniły inaczej. W przypadku rozwiązania umowy na podstawie niniejszej klauzuli zastosowanie ma klauzula 16 lit. d) i e).

Klauzula 15

Obowiązki podmiotu odbierającego dane w przypadku dostępu przez organy publiczne

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*(w przypadku gdy podmiot przetwarzający z UE łączy dane osobowe otrzymane od administratora z państwa trzeciego z danymi osobowymi zgromadzonym przez administratora w UE)*

([12]) Jeżeli chodzi o wpływ takich przepisów i praktyk na zgodność z niniejszymi klauzulami, w ogólnej ocenie można wziąć pod uwagę różne elementy. Do elementów takich można zaliczyć odpowiednie i udokumentowane praktyczne doświadczenie w związku z wcześniejszymi przypadkami żądania przez organy publiczne ujawnienia danych lub brakiem takich żądań, obejmujące wystarczająco reprezentatywne ramy czasowe. Dotyczy to w szczególności wewnętrznych rejestrów lub innych dokumentów, sporządzanych na bieżąco zgodnie z zasadą należytej staranności i certyfikowanych przez kadrę kierowniczą wyższego szczebla, pod warunkiem że informacje te mogą być zgodnie z prawem udostępniane stronom trzecim. Jeżeli takie praktyczne doświadczenie stanowi podstawę do stwierdzenia, że podmiot odbierający dane nie będzie miał utrudnionej możliwości przestrzegania niniejszych klauzul, musi być ono poparte innymi istotnymi, obiektywnymi elementami i to do Stron należy staranne rozważenie, czy elementy te łącznie są wystarczająco istotne pod względem ich wiarygodności i reprezentatywności, aby potwierdzić takie stwierdzenie. W szczególności Strony muszą wziąć pod uwagę, czy ich praktyczne doświadczenie jest potwierdzone i czy nie zaprzeczają mu publicznie udostępnione lub w inny sposób dostępne wiarygodne informacje na temat występowania lub braku żądań w tym samym sektorze lub stosowania prawa w praktyce, takie jak orzecznictwo i sprawozdania sporządzone przez niezależne organy nadzoru.

15.1. **Powiadomienie**

a) Podmiot odbierający dane zobowiązuje się do niezwłocznego powiadomienia podmiotu przekazującego dane oraz, o ile to możliwe, osoby, której dane dotyczą (w stosownych przypadkach z pomocą podmiotu przekazującego dane), jeśli:

(i) otrzyma od organu publicznego, w tym sądowego, prawnie wiążące żądanie – zgodnie z przepisami państwa przeznaczenia – ujawnienia danych osobowych przekazywanych na podstawie niniejszych klauzul; takie powiadomienie zawiera informacje na temat danych osobowych, których dotyczy żądanie, organu występującego z żądaniem, podstawy prawnej żądania oraz udzielonej odpowiedzi; lub

(ii) dowie się o jakimkolwiek przypadku bezpośredniego dostępu przez organy publiczne do danych osobowych przekazywanych na podstawie niniejszych klauzul zgodnie z przepisami państwa przeznaczenia; takie powiadomienie zawiera wszelkie informacje, do których podmiot odbierający dane ma dostęp.

[W przypadku modułu trzeciego: Podmiot przekazujący dane przekazuje to powiadomienie administratorowi.]

b) Jeżeli podmiotowi odbierającemu dane zakazano powiadamiania podmiotu przekazującego dane lub osoby, której dane dotyczą, na mocy przepisów państwa przeznaczenia, zgadza się on dołożyć wszelkich starań, aby uzyskać zwolnienie z tego zakazu w celu przekazania jak największej ilości informacji w jak najkrótszym czasie. Podmiot odbierający dane zgadza się udokumentować swoje starania, aby móc je wykazać na żądanie podmiotu przekazującego dane.

c) Jeżeli jest to dopuszczalne zgodnie z przepisami państwa przeznaczenia, podmiot odbierający dane zgadza się dostarczać podmiotowi przekazującemu dane, w regularnych odstępach czasu w okresie obowiązywania umowy, jak najwięcej istotnych informacji o otrzymanych żądaniach (w szczególności na temat liczby żądań, rodzaju wymaganych danych, organu lub organów występujących z żądaniem, a także informacji o tym, czy żądania były przedmiotem środków zaradczych służących ich zakwestionowaniu i jaki był wynik takich działań itp.). [W przypadku modułu trzeciego: Podmiot przekazujący dane przekazuje te informacje administratorowi.]

d) Podmiot odbierający dane zgadza się przechowywać informacje, o których mowa w lit. a)–c), przez okres obowiązywania umowy i udostępniać je na żądanie właściwego organu nadzorczego.

e) Lit. a)–c) pozostają bez uszczerbku dla obowiązku podmiotu odbierającego dane wynikającego z klauzuli 14 lit. e) i klauzuli 16, dotyczącego niezwłocznego poinformowania podmiotu przekazującego dane, w przypadku gdy nie może on zapewnić zgodności z postanowieniami niniejszych klauzul.

15.2. **Kontrola legalności i minimalizacja danych**

a) Podmiot odbierający dane zgadza się skontrolować legalność żądania ujawnienia danych, a w szczególności kwestii, czy mieści się ono w zakresie uprawnień przyznanych organowi publicznemu występującemu z żądaniem, oraz zakwestionować ważność żądania, jeżeli po dokonaniu starannej oceny stwierdzi, że istnieją uzasadnione podstawy do uznania, iż żądanie jest niezgodne z prawem w świetle przepisów państwa przeznaczenia, mających zastosowanie zobowiązań wynikających z prawa międzynarodowego i zasad kurtuazji międzynarodowej. Podmiot odbierający dane korzysta z możliwości odwołania się na tych samych warunkach. Kwestionując żądanie, podmiot odbierający dane dąży do zastosowania środków tymczasowych w celu zawieszenia skutków żądania do czasu rozstrzygnięcia istoty sprawy przez właściwy organ sądowy. Nie może ujawniać danych osobowych, których dotyczy żądanie, dopóki nie będzie do tego zobowiązany na mocy mających zastosowanie przepisów procesowych. Wymogi te pozostają bez uszczerbku dla obowiązków podmiotu odbierającego dane wynikających z klauzuli 14 lit. e).

b) Podmiot odbierający dane zgadza się udokumentować swoją ocenę prawną, a także wszelkie przypadki zakwestionowania żądania ujawnienia danych oraz, w zakresie dopuszczalnym przez przepisy państwa przeznaczenia, udostępnić dokumentację podmiotowi przekazującemu dane. Udostępnia ją również na żądanie właściwego organu nadzorczego. [W przypadku modułu trzeciego: Podmiot przekazujący dane udostępnia wyniki oceny administratorowi.]

c) Podmiot odbierający dane zgadza się dostarczyć minimalną dopuszczalną ilość informacji, udzielając odpowiedzi na żądanie ujawnienia danych, w oparciu o jego rozsądną interpretację.

SEKCJA IV – POSTANOWIENIA KOŃCOWE

Klauzula 16

Brak zgodności z klauzulami i rozwiązanie umowy

a) Podmiot odbierający dane niezwłocznie informuje podmiot przekazujący dane, jeżeli z jakiegokolwiek powodu nie może zapewnić przestrzegania postanowień niniejszych klauzul.

b) W przypadku gdy podmiot odbierający dane narusza postanowienia niniejszych klauzul lub nie może zapewnić przestrzegania ich postanowień, podmiot przekazujący dane czasowo, do chwili ponownego zapewnienia przestrzegania klauzul lub rozwiązania umowy, wstrzymuje przekazywanie danych osobowych do podmiotu odbierającego. Powyższe pozostaje bez uszczerbku dla postanowień klauzuli 14 lit. f).

c) Podmiot przekazujący dane jest uprawniony do rozwiązania umowy – o ile problem dotyczy przetwarzania danych osobowych na podstawie niniejszych klauzul – w przypadku gdy:

   (i) podmiot przekazujący dane wstrzymał przekazywanie danych osobowych do podmiotu odbierającego dane na podstawie lit. b), a zgodność z postanowieniami niniejszych klauzul nie została przywrócona w rozsądnym terminie, a w każdym razie w ciągu jednego miesiąca od wstrzymania;

   (ii) podmiot odbierający dane w poważnym stopniu lub uporczywie narusza postanowienia niniejszych klauzul; lub

   (iii) podmiot odbierający dane nie zastosował się do wiążącej decyzji właściwego sądu lub organu nadzorczego dotyczącej jego obowiązków wynikających z niniejszych klauzul.

   W takich przypadkach informuje on właściwy organ nadzorczy [w przypadku modułu trzeciego: oraz administratora] o takim przypadku niezastosowania się do decyzji. W przypadku gdy umowa dotyczy więcej niż dwóch Stron, podmiot przekazujący dane może skorzystać z tego prawa do rozwiązania umowy tylko w odniesieniu do odpowiedniej Strony, chyba że Strony uzgodniły inaczej.

d) [W przypadku modułów pierwszego, drugiego i trzeciego: Dane osobowe przekazane przed rozwiązaniem umowy na podstawie lit. c) muszą zostać – w zależności od wyboru dokonanego przez podmiot przekazujący dane – niezwłocznie zwrócone temu podmiotowi lub w całości usunięte. To samo dotyczy wszelkich kopii tych danych.] [W przypadku modułu czwartego: Dane osobowe zgromadzone przez podmiot przekazujący dane w UE, które zostały przekazane przed rozwiązaniem umowy na podstawie lit. c), a także wszelkie ich kopie, muszą niezwłocznie zostać w całości usunięte.] Podmiot odbierający dane poświadcza usunięcie danych podmiotowi przekazującemu. Do czasu usunięcia lub zwrotu danych podmiot odbierający dane nadal zapewnia zgodność z niniejszymi klauzulami. Jeżeli lokalne prawo obowiązujące podmiot odbierający dane zabrania zwrotu lub usunięcia przekazanych danych osobowych, podmiot odbierający dane gwarantuje, że będzie w dalszym ciągu zapewniał przestrzeganie niniejszych klauzul oraz że będzie przetwarzał dane wyłącznie w zakresie i w czasie wymaganym przez to prawo lokalne.

e) Każda ze Stron może wycofać swoją zgodę na związanie się niniejszymi klauzulami, w przypadku gdy: (i) Komisja Europejska przyjmie decyzję na podstawie art. 45 ust. 3 rozporządzenia (UE) 2016/679 obejmującą przekazywanie danych osobowych, do których mają zastosowanie niniejsze klauzule; lub (ii) rozporządzenie (UE) 2016/679 stanie się częścią ram prawnych państwa, do którego przekazywane są dane osobowe. Powyższe pozostaje bez uszczerbku dla pozostałych obowiązków mających zastosowanie do przedmiotowego przetwarzania na podstawie rozporządzenia (UE) 2016/679.

Klauzula 17

Prawo właściwe

MODUŁ PIERWSZY: Przekazywanie między administratorami

MODUŁ DRUGI: Przekazywanie przez administratora podmiotowi przetwarzającemu

MODUŁ TRZECI: Przekazywanie między podmiotami przetwarzającymi

[WARIANT 1: Niniejsze klauzule podlegają przepisom prawa jednego z państw członkowskich UE, pod warunkiem że prawo to dopuszcza prawa osób trzecich, na rzecz których zawarto umowę. Strony uzgadniają, że jest to prawo obowiązujące na terytorium _____ (*należy wskazać państwo członkowskie*).]

[WARIANT 2 (w przypadku modułów drugiego i trzeciego): Niniejsze klauzule podlegają przepisom prawa państwa członkowskiego UE, w którym podmiot przekazujący dane posiada jednostkę organizacyjną. W przypadku gdy przepisy te nie dopuszczają praw osób trzecich, na rzecz których zawarto umowę, podlegają one przepisom prawa innego państwa członkowskiego UE, które dopuszczają prawa osób trzecich, na rzecz których zawarto umowę. Strony uzgadniają, że jest to prawo obowiązujące na terytorium _____ (*należy wskazać państwo członkowskie*).]

MODUŁ CZWARTY: Przekazywanie przez podmiot przetwarzający administratorowi

Niniejsze klauzule podlegają przepisom prawa państwa, które dopuszcza prawa osób trzecich, na rzecz których zawarto umowę. Strony uzgadniają, że jest to prawo obowiązujące na terytorium _____ (*należy wskazać państwo*).

Klauzula 18

Wybór forum i jurysdykcji

MODUŁ PIERWSZY: Przekazywanie między administratorami

MODUŁ DRUGI: Przekazywanie przez administratora podmiotowi przetwarzającemu

MODUŁ TRZECI: Przekazywanie między podmiotami przetwarzającymi

a) Wszelkie spory wynikające z niniejszych klauzul są rozstrzygane przez sądy państwa członkowskiego UE.

b) Strony uzgadniają, że są to sądy _____ (*należy wskazać państwo członkowskie*).

c) Osoba, której dane dotyczą, może również wszcząć postępowanie sądowe przeciwko podmiotowi przekazującemu dane lub podmiotowi odbierającemu dane przed sądami państwa członkowskiego, w którym znajduje się jej miejsce zwykłego pobytu.

d) Strony uzgadniają, że będą podlegały jurysdykcji tych sądów.

MODUŁ CZWARTY: Przekazywanie przez podmiot przetwarzający administratorowi

Wszelkie spory wynikające z niniejszych klauzul są rozstrzygane przez sądy _____ (*należy wskazać państwo*).

DODATEK

UWAGA WYJAŚNIAJĄCA:

Musi istnieć możliwość wyraźnego rozróżnienia informacji mających zastosowanie do każdego przekazania lub kategorii przekazywania oraz, w związku z tym, określenia odnośnych ról stron jako podmiotów przekazujących dane lub podmiotów odbierających dane. Nie jest konieczne wypełnienie i podpisanie oddzielnych dodatków dla każdego przekazania/kategorii przekazywania lub stosunku umownego, w przypadku gdy przejrzystość można uzyskać za pomocą jednego dodatku. W przypadkach, w których konieczne jest zapewnienia jasności, należy jednak stosować oddzielne dodatki.

ZAŁĄCZNIK I

A. **WYKAZ STRON**

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

Podmiot(y) przekazujący(-e) dane: [*Dane identyfikujące i dane kontaktowe podmiotu(-ów) przekazującego(-ych) dane oraz w stosownych przypadkach jego/ich inspektora ochrony danych lub przedstawiciela w Unii Europejskiej]*

1. Nazwa: ……

   Adres: ……

   Imię i nazwisko, stanowisko i dane kontaktowe osoby wyznaczonej do kontaktów: ……

   Działania mające znaczenie dla danych przekazywanych na podstawie niniejszych klauzul: ……

   Podpis i data: ……

   Rola (administrator/podmiot przetwarzający): ……

2. ……

Podmiot(y) odbierający(-e) dane: [*Dane identyfikujące i dane kontaktowe podmiotu(-ów) odbierającego(-ych) dane, w tym każdej osoby wyznaczonej do kontaktów odpowiedzialnej za ochronę danych]*

1. Nazwa: ……

   Adres: ……

   Imię i nazwisko, stanowisko i dane kontaktowe osoby wyznaczonej do kontaktów: ……

   Działania mające znaczenie dla danych przekazywanych na podstawie niniejszych klauzul: ……

   Podpis i data: ……

   Rola (administrator/podmiot przetwarzający): ……

2. ……

B. **OPIS PRZEKAZYWANIA DANYCH**

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

Kategorie osób, których dane dotyczą i których dane są przekazywane

……

Kategorie przekazywanych danych osobowych

……

Przekazywane dane wrażliwe (w stosownych przypadkach) oraz stosowane ograniczenia lub zabezpieczenia, które w pełni uwzględniają charakter danych i związane z nim ryzyko, takie jak na przykład ścisłe ograniczenie celu, ograniczenia dostępu (w tym dostęp wyłącznie dla pracowników, który odbyli specjalistyczne szkolenie), przechowywanie zapisów przypadków udostępnienia danych, ograniczenia dalszego przekazywania lub dodatkowe środki bezpieczeństwa

……

Częstotliwość przekazywania danych (np. czy dane są przekazywane jednorazowo, czy w sposób ciągły)

……

Charakter przetwarzania

.....

Cel(e) przekazywania danych i dalszego przetwarzania

.....

Okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu

.....

W przypadku przekazywania podwykonawcom przetwarzania należy również określić przedmiot, charakter i czas trwania przetwarzania

.....

C. **WŁAŚCIWY ORGAN NADZORCZY**

MODUŁ PIERWSZY: Przekazywanie między administratorami

MODUŁ DRUGI: Przekazywanie przez administratora podmiotowi przetwarzającemu

MODUŁ TRZECI: Przekazywanie między podmiotami przetwarzającymi

Należy określić właściwy organ nadzorczy/organy nadzorcze zgodnie z klauzulą 13

.....

ZAŁĄCZNIK II

ŚRODKI TECHNICZNE I ORGANIZACYJNE, W TYM ŚRODKI TECHNICZNE I ORGANIZACYJNE MAJĄCE NA CELU ZAPEWNIENIE BEZPIECZEŃSTWA DANYCH

MODUŁ PIERWSZY: Przekazywanie między administratorami
MODUŁ DRUGI: Przekazywanie przez administratora podmiotowi przetwarzającemu
MODUŁ TRZECI: Przekazywanie między podmiotami przetwarzającymi

UWAGA WYJAŚNIAJĄCA:

Środki techniczne i organizacyjne muszą być opisane w sposób szczegółowy (a nie ogólny). Zob. również ogólna uwaga na pierwszej stronie dodatku, w szczególności w odniesieniu do potrzeby wyraźnego wskazania, które środki mają zastosowanie do każdego jednorazowego lub wielokrotnego przekazania.

Opis środków technicznych i organizacyjnych wdrożonych przez podmiot(y) odbierający(-e) dane (w tym odpowiednich certyfikacji) w celu zapewnienia odpowiedniego poziomu ochrony, biorąc pod uwagę charakter, zakres, kontekst i cel przetwarzania oraz ryzyko dla praw i wolności osób fizycznych.

[Przykłady ewentualnych środków:

Środki dotyczące pseudonimizacji i szyfrowania danych osobowych

Środki mające na celu ciągłe zapewnienie poufności, integralności, dostępności i odporności systemów i usług przetwarzania

Środki mające na celu zapewnienie zdolności szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego

Procedury regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania

Środki identyfikacji i autoryzacji użytkowników

Środki ochrony danych podczas przekazywania

Środki ochrony danych podczas przechowywania

Środki mające na celu zapewnienie bezpieczeństwa fizycznego miejsc, w których odbywa się przetwarzanie danych osobowych

Środki mające na celu zapewnienie ewidencji zdarzeń

Środki mające na celu zapewnienie konfiguracji systemu, w tym konfiguracji domyślnej

Środki wewnętrznego zarządzania i kierowania w zakresie technologii informacji i bezpieczeństwa informatycznego

Środki certyfikacji/zapewnienia procesów i produktów

Środki mające na celu zapewnienie minimalizacji danych

Środki mające na celu zapewnienie jakości danych

Środki mające na celu zapewnienie ograniczonego zatrzymywania danych

Środki mające na celu zapewnienie odpowiedzialności

Środki mające na celu umożliwienie przenoszenia danych]

W przypadku przekazywania danych podmiotom przetwarzającym (lub podwykonawcom przetwarzania) należy również opisać konkretne środki techniczne i organizacyjne, które ma zastosować ten podmiot lub podwykonawca, aby móc udzielać pomocy administratorowi, a w przypadku przekazywania danych od podmiotu przetwarzającego do podwykonawczy – podmiotowi przekazującemu dane.

ZAŁĄCZNIK III

WYKAZ PODWYKONAWCÓW PRZETWARZANIA

MODUŁ DRUGI: Przekazywanie przez administratora podmiotowi przetwarzającemu
MODUŁ TRZECI: Przekazywanie między podmiotami przetwarzającymi

UWAGA WYJAŚNIAJĄCA:

Niniejszy załącznik wymaga uzupełniania o moduły drugi i trzeci w przypadku szczególnego upoważnienia podwykonawców przetwarzania (klauzula 9 lit. a), wariant 1).

Administrator zezwolił na korzystanie z usług następujących podwykonawców przetwarzania:

1. Nazwa: ……
   Adres: ……
   Imię i nazwisko, stanowisko i dane kontaktowe osoby wyznaczonej do kontaktów: ……
   Opis przetwarzania (w tym wyraźnie rozgraniczenie obowiązków, jeżeli upoważnionych jest kilku podwykonawców przetwarzania): ……
2. ……

DECYZJA WYKONAWCZA KOMISJI (UE) 2021/915

z dnia 4 czerwca 2021 r.

w sprawie standardowych klauzul umownych między administratorami a podmiotami przetwarzającymi na podstawie art. 28 ust. 7 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 oraz art. 29 ust. 7 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725

(Tekst mający znaczenie dla EOG)

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając 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 („rozporządzenie (UE) 2016/679") [1], w szczególności jego art. 28 ust. 7,

uwzględniając 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 („rozporządzenie (UE) 2018/1725") [2], w szczególności jego art. 29 ust. 7,

a także mając na uwadze, co następuje:

(1) Pojęcia administratora i podmiotu przetwarzającego odgrywają kluczową rolę w stosowaniu rozporządzenia (UE) 2016/679 i rozporządzenia (UE) 2018/1725. „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. Do celów rozporządzenia (UE) 2018/1725 administrator oznacza instytucję lub organ Unii lub dyrekcję generalną lub jakąkolwiek inną jednostkę organizacyjną, która samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. Jeżeli cele i sposoby takiego przetwarzania są określone w konkretnym akcie unijnym, Unia może wyznaczyć administratora lub określić konkretne kryteria jego wyznaczania. „Podmiot przetwarzający" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora.

(2) Do relacji między administratorami danych a podmiotami przetwarzającymi dane podlegającymi rozporządzeniu (UE) 2016/679 powinien mieć zastosowanie ten sam zestaw standardowych klauzul umownych – również gdy administratorzy i podmioty przetwarzające podlegają rozporządzeniu (UE) 2018/1725. Wynika to z faktu, że w celu zapewnienia spójnego podejścia do ochrony danych osobowych w całej Unii oraz swobodnego przepływu danych osobowych w Unii, przepisy o ochronie danych zawarte w rozporządzeniu (UE) 2016/679, mające zastosowanie do sektora publicznego w państwach członkowskich, oraz przepisy o ochronie danych zawarte w rozporządzeniu (UE) 2018/1725, mające zastosowanie do instytucji, organów i jednostek organizacyjnych Unii, dostosowano wzajemnie w jak największym stopniu.

(3) Aby zapewnić przestrzeganie wymogów rozporządzeń (UE) 2016/679 i (UE) 2018/1725, administrator powinien, powierzając podmiotowi przetwarzającemu dane czynności przetwarzania, korzystać wyłącznie z usług podmiotów przetwarzających, które zapewniają wystarczające gwarancje – w szczególności jeżeli chodzi o wiedzę fachową, wiarygodność i zasoby – wdrożenia środków technicznych i organizacyjnych, które spełniają wymogi rozporządzenia (UE) 2016/679 i rozporządzenia (UE) 2018/1725, w tym wymogi bezpieczeństwa przetwarzania.

(4) Przetwarzanie przez podmiot przetwarzający powinno odbywać się na podstawie umowy lub innego aktu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i administratora oraz określają elementy wymienione w art. 28 ust. 3 i 4 rozporządzenia (UE) 2016/679 lub w art. 29 ust. 3 i 4 rozporządzenia (UE) 2018/1725. Umowa lub akt ma formę pisemną, w tym formę elektroniczną.

(5) Zgodnie z art. 28 ust. 6 rozporządzenia (UE) 2016/679 i art. 29 ust. 6 rozporządzenia (UE) 2018/1725 administrator i podmiot przetwarzający mogą podjąć decyzję o wynegocjowaniu indywidualnej umowy zawierającej obowiązkowe elementy określone odpowiednio w art. 28 ust. 3 i 4 rozporządzenia (UE) 2016/679 lub w art. 29 ust. 3 i 4 rozporządzenia (UE) 2018/1725 lub o stosowaniu, w całości lub w części, standardowych klauzul umownych przyjętych przez Komisję zgodnie z art. 28 ust. 7 rozporządzenia (UE) 2016/679 i art. 29 ust. 7 rozporządzenia (UE) 2018/1725.

[1] Dz.U. L 119 z 4.5.2016, s. 1.
[2] Dz.U. L 295 z 21.11.2018, s. 39.

(6) Administrator i podmiot przetwarzający powinni mieć swobodę umieszczania standardowych klauzul umownych określonych w niniejszej decyzji w treści umowy o szerszym zakresie oraz dodawania innych klauzul lub dodatkowych zabezpieczeń, pod warunkiem że nie będą one bezpośrednio lub pośrednio sprzeczne ze standardowymi klauzulami umownymi ani nie będą naruszały podstawowych praw lub wolności osób, których dane dotyczą. Stosowanie standardowych klauzul umownych pozostaje bez uszczerbku dla zobowiązań umownych administratora lub podmiotu przetwarzającego do zapewnienia poszanowania obowiązujących przywilejów i immunitetów.

(7) Standardowe klauzule umowne powinny obejmować zarówno przepisy materialne, jak i proceduralne. W art. 28 ust. 3 rozporządzenia (UE) 2016/679 i art. 29 ust. 3 rozporządzenia (UE) 2018/1725 określono, że standardowe klauzule umowne powinny również zobowiązywać administratora i podmiot przetwarzający do określenia przedmiotu i czasu trwania przetwarzania, jego charakteru i celu, rodzaju danych osobowych, kategorii osób, których dane dotyczą, oraz obowiązków i praw administratora.

(8) Zgodnie z art. 28 ust. 3 rozporządzenia (UE) 2016/679 i art. 29 ust. 3 rozporządzenia (UE) 2018/1725 podmiot przetwarzający powinien niezwłocznie poinformować administratora, jeżeli jego zdaniem polecenie wydane mu przez administratora stanowi naruszenie rozporządzenia (UE) 2016/679 lub rozporządzenia (UE) 2018/1725 lub innych przepisów Unii lub państwa członkowskiego o ochronie danych.

(9) Jeżeli podmiot przetwarzający korzysta z usług innego podmiotu przetwarzającego przy wykonywaniu określonych czynności, zastosowanie powinny mieć szczególne wymogi, o których mowa w art. 28 ust. 2 i 4 rozporządzenia (UE) 2016/679 lub w art. 29 ust. 2 i 4 rozporządzenia (UE) 2018/1725. W szczególności wymagana jest uprzednia szczegółowa lub ogólna pisemna zgoda administratora. Niezależnie od tego, czy uprzednia zgoda ma charakter szczegółowy czy ogólny, pierwszy podmiot przetwarzający powinien prowadzić aktualny wykaz innych podmiotów przetwarzających.

(10) Aby spełnić wymogi określone w art. 46 ust. 1 rozporządzenia (UE) 2016/679, Komisja przyjęła standardowe klauzule umowne na podstawie art. 46 ust. 2 lit. c) rozporządzenia (UE) 2016/679. Klauzule te spełniają również wymogi określone w art. 28 ust. 3 i 4 rozporządzenia (UE) 2016/679 w odniesieniu do przekazywania danych przez administratorów podlegających rozporządzeniu (UE) 2016/679 podmiotom przetwarzającym nieobjętym zakresem terytorialnym stosowania tego rozporządzenia lub przez podmioty przetwarzające podlegające rozporządzeniu (UE) 2016/679 podmiotom podprzetwarzającym nieobjętym zakresem terytorialnym stosowania tego rozporządzenia. Standardowych klauzul umownych nie można stosować jako standardowych klauzul umownych do celów rozdziału V rozporządzenia (UE) 2016/679.

(11) Osoby trzecie powinny mieć możliwość stania się stroną standardowych klauzul umownych przez cały okres obowiązywania umowy.

(12) Funkcjonowanie standardowych klauzul umownych należy ocenić w ramach okresowej oceny rozporządzenia (UE) 2016/679, o której mowa w art. 97 tego rozporządzenia.

(13) Zgodnie z art. 42 ust. 1 i 2 rozporządzenia (UE) 2018/1725 przeprowadzono konsultacje z Europejskim Inspektorem Ochrony Danych i Europejską Radą Ochrony Danych, które to konsultacje zakończyły się wydaniem wspólnej opinii w dniu 14 stycznia 2021 r. ([3]) Opinia ta została uwzględniona podczas przygotowywania niniejszej decyzji.

(14) Środki przewidziane w niniejszej decyzji są zgodne z opinią komitetu ustanowionego na mocy art. 93 rozporządzenia (UE) 2016/679 i art. 96 ust. 2 rozporządzenia (UE) 2018/1725,

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

Artykuł 1

Standardowe klauzule umowne określone w załączniku spełniają wymogi dotyczące umów zawieranych między administratorami a podmiotami przetwarzającymi określone w art. 28 ust. 3 i 4 rozporządzenia (UE) 2016/679 oraz w art. 29 ust. 3 i 4 rozporządzenia (UE) 2018/1725.

Artykuł 2

Standardowe klauzule umowne określone w załączniku można stosować w umowach zawieranych między administratorem a podmiotem przetwarzającym, który przetwarza dane osobowe w jego imieniu.

([3]) 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

Artykuł 3

Komisja ocenia praktyczne stosowanie standardowych klauzul umownych określonych w załączniku na podstawie wszystkich dostępnych informacji w ramach oceny okresowej, o której mowa w art. 97 rozporządzenia (UE) 2016/679.

Artykuł 4

Niniejsza decyzja wchodzi w życie dwudziestego dnia po jej opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

Sporządzono w Brukseli dnia 4 czerwca 2021 r.

W imieniu Komisji
Ursula VON DER LEYEN
Przewodnicząca

ZAŁĄCZNIK

Standardowe klauzule umowne

SEKCJA I

Klauzula 1

Cel i zakres

a) Celem niniejszych standardowych klauzul umownych („klauzule") jest zapewnienie przestrzegania [należy wybrać odpowiednią opcję: OPCJA 1: art. 28 ust. 3 i 4 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)] / [OPCJA 2: art. 29 ust. 3 i 4 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 oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE].

b) Administratorzy i podmioty przetwarzające wymienieni w załączniku I uzgodnili niniejsze klauzule w celu zapewnienia przestrzegania art. 28 ust. 3 i 4 rozporządzenia (UE) 2016/679 lub art. 29 ust. 3 i 4 rozporządzenia (UE) 2018/1725.

c) Niniejsze klauzule mają zastosowanie do przetwarzania danych osobowych określonego w załączniku II.

d) Załączniki I–IV stanowią integralną część klauzul.

e) Niniejsze klauzule pozostają bez uszczerbku dla obowiązków, którym podlega administrator danych na mocy rozporządzenia (UE) 2016/679 lub rozporządzenia (UE) 2018/1725.

f) Niniejsze klauzule same w sobie nie zapewniają wypełnienia obowiązków związanych z międzynarodowym przekazywaniem danych zgodnie z rozdziałem V rozporządzenia (UE) 2016/679 lub rozporządzenia (UE) 2018/1725.

Klauzula 2

Niezmienność klauzul

a) Strony zobowiązują się nie zmieniać klauzul z wyjątkiem dodawania informacji do załączników lub aktualizowania zawartych w nich informacji.

b) Postanowienie to nie uniemożliwia stronom umieszczania standardowych klauzul umownych określonych w niniejszych klauzulach w treści umowy o szerszym zakresie ani dodawania innych klauzul lub dodatkowych zabezpieczeń, pod warunkiem że nie będą one bezpośrednio lub pośrednio sprzeczne z klauzulami umownymi ani nie będą naruszały podstawowych praw lub wolności osób, których dane dotyczą.

Klauzula 3

Wykładnia

a) Jeżeli w niniejszych klauzulach użyto terminów zdefiniowanych odpowiednio w rozporządzeniu (UE) 2016/679 lub rozporządzeniu (UE) 2018/1725, terminy te mają takie samo znaczenie jak w tych rozporządzeniach.

b) Niniejsze klauzule odczytuje się i interpretuje w świetle odpowiednio przepisów rozporządzenia (UE) 2016/679 lub rozporządzenia (UE) 2018/1725.

c) Niniejszych klauzul nie interpretuje się w sposób sprzeczny z prawami i obowiązkami przewidzianymi w rozporządzeniu (UE) 2016/679 lub rozporządzeniu (UE) 2018/1725 ani w sposób naruszający podstawowe prawa lub wolności osób, których dane dotyczą.

Klauzula 4

Hierarchia

W razie sprzeczności między niniejszymi klauzulami a postanowieniami powiązanych umów między stronami istniejących w chwili uzgadniania niniejszych klauzul lub zawartych po ich uzgodnieniu, pierwszeństwo mają niniejsze klauzule.

Klauzula 5 – fakultatywna

Klauzula przystąpienia

a) Każdy podmiot niebędący stroną niniejszych klauzul może za zgodą wszystkich stron przystąpić do niniejszych klauzul jako administrator lub podmiot przetwarzający w dowolnym czasie, wypełniając załączniki i podpisując załącznik I.

b) Po wypełnieniu i podpisaniu załączników wymienionych w lit. a) podmiot przystępujący jest traktowany jako strona niniejszych klauzul i ma prawa i obowiązki administratora lub podmiotu przetwarzającego, zgodnie z rolą nadaną mu w załączniku I.

c) Przed przystąpieniem do niniejszych klauzul jako ich strona podmiot przystępujący nie ma żadnych praw ani obowiązków wynikających z niniejszych klauzul.

SEKCJA II

OBOWIĄZKI STRON

Klauzula 6

Opis przetwarzania

Szczegóły dotyczące operacji przetwarzania, w szczególności kategorie danych osobowych i cele, dla których dane osobowe są przetwarzane w imieniu administratora, określono w załączniku II.

Klauzula 7

Obowiązki stron

7.1. **Polecenia**

a) 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 nie zabrania udzielenia takiej informacji z uwagi na ważny interes publiczny. Administrator może wydawać kolejne polecenia przez cały okres przetwarzania danych osobowych. Polecenia te są zawsze dokumentowane.

b) Podmiot przetwarzający bezzwłocznie powiadamia administratora, jeżeli w opinii podmiotu przetwarzającego polecenie wydane przez administratora narusza rozporządzenie (UE) 2016/679 lub rozporządzenie (UE) 2018/1725 lub obowiązujące przepisy Unii lub państwa członkowskiego o ochronie danych.

7.2. **Ograniczenie celu**

Podmiot przetwarzający przetwarza dane osobowe wyłącznie w konkretnym celu lub celach przetwarzania, określonych w załączniku II, chyba że otrzyma dalsze polecenia od administratora.

7.3. **Czas trwania przetwarzania danych osobowych**

Przetwarzanie przez podmiot przetwarzający odbywa się wyłącznie przez okres określony w załączniku II.

7.4. **Bezpieczeństwo przetwarzania**

a) W celu zapewnienia bezpieczeństwa danych osobowych podmiot przetwarzający wdraża co najmniej środki techniczne i organizacyjne określone w załączniku III. Zapewnienie bezpieczeństwa danych obejmuje ochronę danych przed naruszeniem bezpieczeństwa prowadzącym do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych (naruszenie ochrony danych osobowych). Oceniając odpowiedni poziom bezpieczeństwa, strony należycie uwzględniają stan wiedzy technicznej, koszty wdrażania, charakter, zakres, kontekst i cele przetwarzania oraz związane z tym ryzyko dla osób, których dane dotyczą.

b) Podmiot przetwarzający udziela członkom swojego personelu dostępu do danych osobowych podlegających przetwarzaniu jedynie w zakresie bezwzględnie niezbędnym do wykonania umowy, zarządzania nią i jej monitorowania. Podmiot przetwarzający zapewnia, by osoby upoważnione do przetwarzania otrzymanych danych osobowych zobowiązały się do zachowania poufności lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania poufności.

7.5. **Dane wrażliwe**

Jeżeli przetwarzanie obejmuje dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne lub dane biometryczne do celów jednoznacznego zidentyfikowania osoby fizycznej, dane dotyczące zdrowia, seksualności lub orientacji seksualnej danej osoby, bądź dane dotyczące wyroków skazujących i czynów zabronionych („dane wrażliwe"), podmiot przetwarzający stosuje szczególne ograniczenia lub dodatkowe zabezpieczenia.

7.6. **Dokumentacja i zgodność**

a) Strony są w stanie wykazać zgodność z niniejszymi klauzulami.

b) Podmiot przetwarzający niezwłocznie i odpowiednio rozpatruje zapytania administratora dotyczące przetwarzania danych zgodnie z niniejszymi klauzulami.

c) Podmiot przetwarzający udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków, które są określone w niniejszych klauzulach i wynikają bezpośrednio z rozporządzenia (UE) 2016/679 lub rozporządzenia (UE) 2018/1725. Na wniosek administratora podmiot przetwarzający zezwala również na audyty czynności przetwarzania objętych niniejszymi klauzulami i uczestniczy w tych audytach. Audyty te przeprowadza się w rozsądnych odstępach czasu lub jeżeli istnieją przesłanki wskazujące na niezgodność. Podejmując decyzję w sprawie przeglądu lub audytu, administrator może wziąć pod uwagę odpowiednie certyfikaty, jakie ma podmiot przetwarzający.

d) Administrator może przeprowadzić audyt samodzielnie lub upoważnić do jego przeprowadzenia niezależnego audytora. Audyty mogą również obejmować inspekcje w pomieszczeniach lub obiektach fizycznych podmiotu przetwarzającego. Audyty te przeprowadza się, informując o nich, w stosownych przypadkach, z odpowiednim wyprzedzeniem.

e) Na wniosek właściwego(-ych) organu(-ów) nadzorczego(-ych) strony udostępniają mu (im) informacje, o których mowa w niniejszej klauzuli, w tym wyniki wszelkich audytów.

7.7. **Korzystanie z usług podmiotów podprzetwarzających**

a) OPCJA 1: UPRZEDNIA SZCZEGÓŁOWA ZGODA: Podmiot przetwarzający nie może podzlecać żadnych operacji przetwarzania dokonywanych w imieniu administratora zgodnie z niniejszymi klauzulami podmiotowi podprzetwarzającemu bez uprzedniej szczegółowej pisemnej zgody administratora. Podmiot przetwarzający składa wniosek o udzielenie szczegółowej zgody co najmniej [NALEŻY PODAĆ TERMIN] przed rozpoczęciem korzystania z usług danego podmiotu podprzetwarzającego wraz z informacjami niezbędnymi do tego, by administrator mógł podjąć decyzję w sprawie zgody. Załącznik IV zawiera wykaz podmiotów podprzetwarzających upoważnionych przez administratora. Strony są obowiązane do aktualizacji załącznika IV.

OPCJA 2: OGÓLNA PISEMNA ZGODA: Podmiot przetwarzający ma ogólną zgodę administratora na korzystanie z usług podmiotów podprzetwarzających wpisanych do uzgodnionego wykazu. Podmiot przetwarzający informuje administratora na piśmie o wszelkich zamierzonych zmianach w tym wykazie polegających na dodaniu lub zastąpieniu podmiotów podprzetwarzających z wyprzedzeniem co najmniej [NALEŻY PODAĆ TERMIN], dając tym samym administratorowi wystarczająco dużo czasu na wyrażenie sprzeciwu wobec takich zmian przed rozpoczęciem korzystania z usług danego podmiotu podprzetwarzającego (podmiotów podprzetwarzających). Podmiot przetwarzający przekazuje administratorowi niezbędne informacje umożliwiające mu skorzystanie z prawa sprzeciwu.

b) Jeżeli podmiot przetwarzający korzysta z usług podmiotu podprzetwarzającego w celu przeprowadzenia określonych czynności przetwarzania (w imieniu administratora), dokonuje tego w drodze umowy, która nakłada na podmiot podprzetwarzający zasadniczo takie same obowiązki w zakresie ochrony danych jak obowiązki nałożone na podmiot przetwarzający dane zgodnie z niniejszymi klauzulami. Podmiot przetwarzający zapewnia, aby podmiot podprzetwarzający wypełniał obowiązki, którym podlega podmiot przetwarzający na mocy niniejszych klauzul oraz rozporządzenia (UE) 2016/679 lub rozporządzenia (UE) 2018/1725.

c) Na wniosek administratora podmiot przetwarzający przekazuje administratorowi kopię umowy, jaką zawarł z podmiotem podprzetwarzającym, a w razie wprowadzenia zmian przekazuje administratorowi jej zaktualizowaną wersję. W zakresie niezbędnym do ochrony tajemnicy handlowej lub innych informacji poufnych, w tym danych osobowych, podmiot przetwarzający może utajnić tekst umowy przed jej udostępnieniem.

d) Podmiot przetwarzający pozostaje w pełni odpowiedzialny przed administratorem za wykonanie obowiązków podmiotu podprzetwarzającego zgodnie z jego umową z podmiotem przetwarzającym. Podmiot przetwarzający powiadamia administratora o każdym przypadku niewywiązania się przez podmiot podprzetwarzający z jego zobowiązań umownych.

e) Podmiot przetwarzający uzgadnia z podmiotem podprzetwarzającym klauzulę dotyczącą beneficjenta będącego osobą trzecią, zgodnie z którą to klauzulą – jeżeli podmiot przetwarzający przestanie istnieć faktycznie lub formalnie lub stanie się niewypłacalny – administrator ma prawo rozwiązać umowę z podmiotem podprzetwarzającym i nakazać mu usunięcie lub zwrot danych osobowych.

7.8. **Międzynarodowe przekazywanie danych**

a) Wszelkie przekazywanie danych do państwa trzeciego lub organizacji międzynarodowej przez podmiot przetwarzający odbywa się wyłącznie na udokumentowane polecenie administratora lub w celu spełnienia szczególnego wymogu na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega podmiot przetwarzający, i odbywa się zgodnie z rozdziałem V rozporządzenia (UE) 2016/679 lub rozporządzenia (UE) 2018/1725.

b) Jeżeli zgodnie z klauzulą 7.7 podmiot przetwarzający korzysta z usług podmiotu podprzetwarzającego w celu przeprowadzenia określonych czynności przetwarzania (w imieniu administratora), które wiążą się z przekazywaniem danych osobowych w rozumieniu rozdziału V rozporządzenia (UE) 2016/679, administrator wyraża zgodę na to, by podmioty te mogły zapewnić zgodność z rozdziałem V rozporządzenia (UE) 2016/679 za pomocą standardowych klauzul umownych przyjętych przez Komisję zgodnie z art. 46 ust. 2 rozporządzenia (UE) 2016/679, pod warunkiem że spełnione są warunki stosowania tych standardowych klauzul umownych.

Klauzula 8

Pomoc dla administratora

a) Podmiot przetwarzający niezwłocznie zawiadamia administratora o każdym wniosku otrzymanym od osoby, której dane dotyczą. Podmiot przetwarzający nie odpowiada na taki wniosek samodzielnie, chyba że administrator wyraził na to zgodę.

b) Podmiot przetwarzający pomaga administratorowi w wypełnianiu jego obowiązków dotyczących udzielania odpowiedzi na wnioski osób, których dane dotyczą, o skorzystanie z przysługujących im praw, z uwzględnieniem charakteru przetwarzania. Wypełniając swoje obowiązki zgodnie z lit. a) i b), podmiot przetwarzający stosuje się do poleceń administratora.

c) Oprócz spoczywającego na podmiocie przetwarzającym obowiązku pomagania administratorowi zgodnie z klauzulą 8 lit. b) podmiot przetwarzający pomaga mu ponadto w zapewnieniu wypełniania następujących obowiązków, z uwzględnieniem charakteru przetwarzania danych oraz informacji, którymi dysponuje podmiot przetwarzający:

1) obowiązek przeprowadzenia oceny wpływu planowanych operacji przetwarzania na ochronę danych osobowych („ocena skutków dla ochrony danych"), jeżeli dany rodzaj przetwarzania może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych;

2) obowiązek skonsultowania się z właściwym(-i) organem(-ami) nadzorczym(-i) przed rozpoczęciem przetwarzania, jeżeli ocena skutków dla ochrony danych wskaże, że przetwarzanie powodowałoby wysokie ryzyko, gdyby administrator nie zastosował środków w celu jego ograniczenia;

3) obowiązek zapewnienia prawidłowości i aktualności danych osobowych poprzez niezwłoczne poinformowanie administratora, jeżeli podmiot przetwarzający stwierdzi, że przetwarzane przez niego dane osobowe są nieprawidłowe lub nieaktualne;

4) obowiązki określone w [OPCJA 1] art. 32 rozporządzenia (UE) 2016/679 / [OPCJA 2] art. 33 i 36–38 rozporządzenia (UE) 2018/1725.

d) Strony określają w załączniku III odpowiednie środki techniczne i organizacyjne, za pomocą których podmiot przetwarzający jest zobowiązany pomagać administratorowi w stosowaniu niniejszej klauzuli, jak również zakres wymaganej pomocy.

Klauzula 9

Zgłaszanie naruszenia ochrony danych osobowych

W przypadku naruszenia ochrony danych osobowych podmiot przetwarzający współpracuje z administratorem i pomaga mu w wypełnianiu jego obowiązków wynikających z art. 33 i 34 rozporządzenia (UE) 2016/679 lub, w stosownych przypadkach, z art. 34 i 35 rozporządzenia (UE) 2018/1725, z uwzględnieniem charakteru przetwarzania i informacji, którymi dysponuje podmiot przetwarzający.

9.1. **Naruszenie ochrony danych dotyczące danych przetwarzanych przez administratora**

W przypadku naruszenia ochrony danych osobowych dotyczącego danych przetwarzanych przez administratora podmiot przetwarzający wspomaga administratora:

a) przy zgłaszaniu naruszenia ochrony danych osobowych właściwemu(-ym) organowi(-om) nadzorczemu(-ym) niezwłocznie po tym, jak administrator dowiedział się o naruszeniu, w stosownych przypadkach/(chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych);

b) przy uzyskiwaniu następujących informacji, które zgodnie z [OPCJA 1] art. 33 ust. 3 rozporządzenia (UE) 2016/679 / [OPCJA 2] art. 34 ust. 3 rozporządzenia (UE) 2018/1725 powinny być zawarte w zgłoszeniu administratora i obejmować co najmniej:

   1) charakter danych osobowych, w tym w miarę możliwości kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;

   2) możliwe konsekwencje naruszenia ochrony danych osobowych;

   3) 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.

Jeżeli przekazanie wszystkich tych informacji równocześnie nie jest możliwe, pierwotne zgłoszenie zawiera informacje dostępne w danej chwili, a po uzyskaniu dostępu do dalszych informacji przekazuje się je bez zbędnej zwłoki;

c) przy wypełnianiu – zgodnie z [OPCJA 1] art. 34 rozporządzenia (UE) 2016/679 / [OPCJA 2] art. 35 rozporządzenia (UE) 2018/1725 – obowiązku zawiadomienia bez zbędnej zwłoki osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, jeżeli naruszenie to może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych.

9.2. **Naruszenie ochrony danych dotyczące danych przetwarzanych przez podmiot przetwarzający**

W przypadku naruszenia ochrony danych osobowych dotyczącego danych przetwarzanych przez podmiot przetwarzający podmiot przetwarzający zgłasza naruszenie administratorowi niezwłocznie po tym, jak dowiedział się o naruszeniu. Zgłoszenie to powinno zawierać co najmniej:

a) opis charakteru naruszenia (w tym, w miarę możliwości, kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz wpisów danych, których dotyczy naruszenie);

b) dane punktu kontaktowego, w którym można uzyskać więcej informacji na temat naruszenia ochrony danych osobowych;

c) wskazanie prawdopodobnych konsekwencji naruszenia oraz środków, które zostały lub mają zostać wprowadzone w celu zaradzenia naruszeniu, w tym w celu zminimalizowania jego ewentualnych negatywnych skutków.

Jeżeli przekazanie wszystkich tych informacji równocześnie nie jest możliwe, pierwotne zgłoszenie zawiera informacje dostępne w danej chwili, a po uzyskaniu dostępu do dalszych informacji przekazuje się je bez zbędnej zwłoki.

Strony określają w załączniku III wszystkie inne elementy, które ma przedstawić podmiot przetwarzający, wspomagając administratora w wypełnianiu jego obowiązków określonych w [OPCJA 1] art. 33 i 34 rozporządzenia (UE) 2016/679 / [OPCJA 2] art. 34 i 35 rozporządzenia (UE) 2018/1725.

SEKCJA III

POSTANOWIENIA KOŃCOWE

Klauzula 10

Naruszenie klauzul i rozwiązanie umowy

a) Bez uszczerbku dla przepisów rozporządzenia (UE) 2016/679 lub rozporządzenia (UE) 2018/1725, w przypadku gdy podmiot przetwarzający narusza swoje obowiązki wynikające z niniejszych klauzul, administrator może polecić mu, by zawiesił przetwarzanie danych osobowych do czasu, gdy podmiot przetwarzający zapewni zgodność z niniejszymi klauzulami, lub umowa ulega rozwiązaniu. Podmiot przetwarzający niezwłocznie zawiadamia administratora, jeżeli z jakiegokolwiek powodu nie jest w stanie zastosować się do niniejszych klauzul.

b) Administrator jest uprawniony do rozwiązania umowy w zakresie, w jakim dotyczy ona przetwarzania danych osobowych zgodnie z niniejszymi klauzulami, jeżeli:

1) administrator zawiesił przetwarzanie danych osobowych przez podmiot przetwarzający zgodnie z lit. a) i jeżeli zgodność z niniejszymi klauzulami nie zostanie przywrócona w rozsądnym terminie, a w każdym razie w terminie jednego miesiąca od zawieszenia;

2) podmiot przetwarzający poważnie lub stale narusza niniejsze klauzule lub swoje obowiązki wynikające z rozporządzenia (UE) 2016/679 lub rozporządzenia (UE) 2018/1725;

3) podmiot przetwarzający nie stosuje się do wiążącej decyzji właściwego sądu lub właściwego(-ych) organu(-ów) nadzorczego(-ych) dotyczącej jego obowiązków wynikających z niniejszych klauzul lub z rozporządzenia (UE) 2016/679 lub rozporządzenia (UE) 2018/1725.

c) Podmiot przetwarzający ma prawo rozwiązać umowę w zakresie, w jakim dotyczy ona przetwarzania danych osobowych zgodnie z niniejszymi klauzulami, jeżeli po zawiadomieniu administratora o tym, że jego polecenie narusza obowiązujące wymogi prawne zgodnie z klauzulą 7.1 lit. b), administrator nalega na wypełnienie polecenia.

d) Po rozwiązaniu umowy podmiot przetwarzający, zależnie od decyzji administratora, usuwa wszystkie dane osobowe przetwarzane w imieniu administratora i poświadcza administratorowi, że tego dokonał, lub zwraca administratorowi wszystkie dane osobowe i usuwa istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych. Podmiot przetwarzający zapewnia przestrzeganie niniejszych klauzul do czasu usunięcia lub zwrotu danych.

ZAŁĄCZNIK I

Wykaz stron

Administrator (administratorzy): [*dane identyfikacyjne i kontaktowe administratora (administratorów) oraz, w stosownych przypadkach, inspektora ochrony danych wyznaczonego przez administratora*]

1. Imię i nazwisko lub nazwa: .....

Adres: .....

Imię i nazwisko, stanowisko i dane kontaktowe osoby wyznaczonej do kontaktów: .....

Podpis i data przystąpienia: .....

2.

.....

Podmiot przetwarzający (podmioty przetwarzające): [*dane identyfikacyjne i kontaktowe podmiotu przetwarzającego (podmiotów przetwarzających) oraz, w stosownych przypadkach, inspektora ochrony danych wyznaczonego przez podmiot przetwarzający*]

1. Imię i nazwisko lub nazwa: .....

Adres: .....

Imię i nazwisko, stanowisko i dane kontaktowe osoby wyznaczonej do kontaktów: .....

Podpis i data przystąpienia: .....

2.

.....

ZAŁĄCZNIK II

Opis przetwarzania

Kategorie osób, których dane osobowe są przetwarzane

……

Kategorie przetwarzanych danych osobowych

……

Przetwarzane dane wrażliwe (w stosownych przypadkach) oraz stosowane ograniczenia lub zabezpieczenia, które w pełni uwzględniają charakter danych i związane z nimi zagrożenia, takie jak na przykład ścisłe ograniczenie celu, ograniczenia dostępu (w tym dostęp wyłącznie dla personelu, który odbył specjalistyczne szkolenie), prowadzenie rejestru dostępu do danych, ograniczenia dotyczące dalszego przekazywania danych lub dodatkowe środki bezpieczeństwa.

……

Charakter przetwarzania

……

Cel(e), w którym(-ych) dane osobowe są przetwarzane w imieniu administratora

……

Czas trwania przetwarzania

……

……

W przypadku przetwarzania przez podmioty przetwarzające lub podprzetwarzające należy również określić przedmiot, charakter i czas trwania przetwarzania.

ZAŁĄCZNIK III

Środki techniczne i organizacyjne, w tym środki techniczne i organizacyjne w celu zapewnienia bezpieczeństwa danych

UWAGA WYJAŚNIAJĄCA:

Środki techniczne i organizacyjne należy opisać szczegółowo, a nie w sposób ogólny.

Opis technicznych i organizacyjnych środków bezpieczeństwa wdrożonych przez podmiot przetwarzający (podmioty przetwarzające) (w tym wszelkie stosowne certyfikaty) w celu zapewnienia odpowiedniego poziomu bezpieczeństwa, z uwzględnieniem charakteru, zakresu, kontekstu i celu przetwarzania, a także ryzyka naruszenia praw i wolności osób fizycznych Przykłady możliwych środków:

Środki umożliwiające pseudonimizację i szyfrowanie danych osobowych

Środki zapewniające zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania

Środki zapewniające zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego

Procesy umożliwiające regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania

Środki umożliwiające identyfikację i autoryzację użytkowników

Środki zapewniające ochronę danych w czasie ich przekazywania

Środki zapewniające ochronę danych w czasie ich przechowywania

Środki służące zapewnieniu bezpieczeństwa fizycznego miejsc, w których przetwarzane są dane osobowe

Środki umożliwiające rejestrowanie zdarzeń

Środki służące do konfiguracji systemu, w tym konfiguracji domyślnej

Środki dotyczące zarządzania wewnętrznym systemem IT i bezpieczeństwem IT

Środki dotyczące certyfikacji / zapewnienia jakości procesów i produktów

Środki zapewniające minimalizację danych

Środki zapewniające odpowiednią jakość danych

Środki zapewniające ograniczone zatrzymywanie danych

Środki zapewniające rozliczalność

Środki umożliwiające przenoszenie danych i zapewnienie ich usuwania]

W przypadku przekazywania danych podmiotom przetwarzającym lub podprzetwarzającym należy również opisać konkretne środki techniczne i organizacyjne, jakie powinien zastosować podmiot przetwarzający lub podprzetwarzający, aby móc udzielić pomocy administratorowi.

Opis konkretnych środków technicznych i organizacyjnych, jakie powinien zastosować podmiot przetwarzający, aby móc udzielić pomocy administratorowi

ZAŁĄCZNIK IV

Wykaz podmiotów podprzetwarzających

UWAGA WYJAŚNIAJĄCA:

Niniejszy załącznik należy wypełnić w razie udzielenia szczegółowej zgody na korzystanie z usług podmiotów podprzetwarzających (klauzula 7.7 lit. a), opcja 1).

Administrator zezwolił na korzystanie z usług następujących podmiotów podprzetwarzających:

1. Imię i nazwisko lub nazwa: ……

Adres: ……

Imię i nazwisko, stanowisko i dane kontaktowe osoby wyznaczonej do kontaktów: ……

Opis przetwarzania (w tym jasne określenie zakresu odpowiedzialności w przypadku upoważnienia kilku podmiotów podprzetwarzających): ……

2. ……

Opinia 17/2018

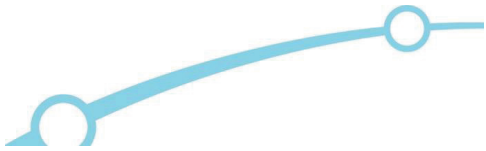
w sprawie projektu wykazu sporządzonego przez właściwy polski organ nadzorczy

dotyczącego

rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych (art. 35 ust. 4 RODO)

przyjęta 25 września 2018 r.

Spis treści



Europejska Rada Ochrony Danych,

uwzględniając art. 63, art. 64 ust. 1 lit. a) i ust. 3–8 oraz art. 35 ust. 1, 3, 4 i 6 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 i protokół 37 do tego Porozumienia, zmienione decyzją Wspólnego Komitetu EOG nr 154/2018 z dnia 6 lipca 2018 r.,

uwzględniając art. 10 i 22 swojego regulaminu z dnia 25 maja 2018 r.,

a także mając na uwadze, co następuje:

(1) Głównym zadaniem Rady jest zapewnienie spójnego stosowania rozporządzenia 2016/679 (zwanego dalej „RODO") na całym terytorium Europejskiego Obszaru Gospodarczego. Zgodnie z art. 64 ust. 1 RODO Rada wydaje opinię, gdy organ nadzorczy zamierza przyjąć wykaz rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych zgodnie z art. 35 ust. 4 rozporządzenia. Celem niniejszej opinii jest zatem ustalenie zharmonizowanego podejścia do przetwarzania, które ma charakter transgraniczny lub może mieć wpływ na swobodny przepływ danych osobowych lub na osobę fizyczną w Unii Europejskiej. Mimo, że RODO nie zawiera jednego wykazu, to nadal propaguje spójność. Rada w swoich opiniach dąży do osiągnięcia tego celu, 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 Rady niekoniecznie stwarzają wysokie ryzyko dla osób, których dane dotyczą, i po trzecie – wzywając te organy do stosowania określonych kryteriów w sposób zharmonizowany.

(2) Zgodnie z art. 35 ust. 4 i 6 RODO właściwe organy nadzorcze sporządzają wykazy rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych. Jeżeli wykazy obejmują jednak operacje 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.

(3) Chociaż projekty wykazów właściwych organów nadzorczych są objęte mechanizmem spójności, nie oznacza to, że wykazy te powinny być identyczne. Właściwe organy nadzorcze mają margines swobody w odniesieniu do kontekstu krajowego lub regionalnego i powinny uwzględniać ustawodawstwo lokalne. Celem oceny/opinii EROD nie jest wypracowanie jednego unijnego wykazu, lecz uniknięcie znaczących niespójności, które mogą mieć wpływ na równoważną ochronę osób, których dane dotyczą.

(4) Zgodnie z art. 35 ust. 1 RODO 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. 35 ust. 3 RODO przedstawiono, co może prowadzić do wystąpienia wysokiego ryzyka. Lista ta nie jest wyczerpująca. Grupa Robocza Art. 29 w Wytycznych dotyczących oceny skutków dla ochrony danych[1], zatwierdzonych przez EROD[2], wyjaśniła kryteria, które mogą pomóc w ustaleniu, kiedy 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 właściwe organy nadzorcze 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. Przy dokonywaniu oceny, czy projekty wykazów sporządzone przez właściwe organy nadzorcze nie mają negatywnego wpływu na spójne stosowanie ogólnego rozporządzenia o ochronie danych, należy zatem stosować kryteria określone w wytycznych Grupy Roboczej Art. 29.

(6) Projekty wykazów zostały przedłożone Europejskiej Radzie Ochrony Danych przez dwadzieścia dwa właściwe organy nadzorcze. Ogólna ocena tych projektów wykazów potwierdza cel, jakim jest spójne stosowanie ogólnego rozporządzenia o ochronie danych, nawet jeżeli zwiększa się złożoność przedmiotowej kwestii.

(7) Opinia EROD zostaje przyjęta zgodnie z art. 64 ust. 3 RODO w związku z art. 10 ust. 2 regulaminu EROD w terminie ośmiu tygodni od pierwszego dnia roboczego po decyzji przewodniczącego i właściwego organu nadzorczego, że dokumentacja jest kompletna. Na podstawie decyzji przewodniczącego termin ten może zostać przedłużony o kolejne sześć tygodni, biorąc pod uwagę złożoność przedmiotu sprawy,

PRZYJMUJE NINIEJSZĄ OPINIĘ:

1. Streszczenie stanu faktycznego

Urząd Ochrony Danych Osobowych (zwany dalej „polskim organem nadzorczym") przedstawił EROD swój projekt wykazu. Decyzję w sprawie kompletności dokumentacji podjęto 20 czerwca 2018 r. Okres, w którym należy przyjąć opinię, został przedłużony do 25 września ze względu na złożoność przedmiotowej kwestii oraz fakt, że dwadzieścia dwa właściwe organy

[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.

nadzorcze przedłożyły projekty wykazów jednocześnie, w związku z czym zaistniała potrzeba przeprowadzenia oceny całościowej.

2. Ocena

2.1 Ogólne uzasadnienie EROD dotyczące przedłożonego wykazu

Każdy wykaz przedłożony EROD został przeanalizowany jako szczegółowe rozwinięcie art. 35 ust. 1, który to przepis zawsze będzie miał znaczenie rozstrzygające. W związku z tym żadnego wykazu nie można uznać za wyczerpujący. Jako że nie zaznaczono tego wyraźnie w wykazie przedstawionym przez polski organ nadzorczy, Rada zwraca się o dodanie tego wyjaśnienia do dokumentu zawierającego wykaz.

Zgodnie z art. 35 ust. 10 RODO Rada jest zdania, że obowiązek dokonania oceny skutków dla ochrony danych zgodnie z art. 35 ust. 1–7 rozporządzenia nie ma zastosowania, jeżeli oceny skutków dla ochrony danych dokonano już w ramach ogólnej oceny skutków regulacji w związku z przyjęciem podstawy prawnej, chyba że dane państwo członkowskie uzna dokonanie oceny skutków dla ochrony danych za niezbędne.

Jeżeli Rada wystąpi ponadto o ocenę skutków dla ochrony danych dotyczącą określonej kategorii przetwarzania, a równoważny środek jest już wymagany w prawie krajowym, polski organ nadzorczy powinien dodać odniesienie do tego środka.

Niniejsza opinia nie obejmuje pozycji przedstawionych przez polski organ nadzorczy, które nie wchodziły w zakres art. 35 ust. 6 RODO. Odnosi się to do pozycji, które nie są związane ani „z oferowaniem towarów lub usług osobom, których dane dotyczą" w kilku państwach członkowskich, ani z monitorowaniem zachowania tych osób w kilku państwach członkowskich. Oprócz tego nie mogą one „znacznie wpłynąć na swobodny przepływ danych osobowych w Unii". Dotyczy to zwłaszcza pozycji odnoszących się do ustawodawstwa krajowego, w szczególności tych, w przypadku których obowiązek dokonania oceny skutków dla ochrony danych jest przewidziany w przepisach krajowych. Uznano ponadto, że wszelkie operacje przetwarzania odnoszące się do egzekwowania prawa nie wchodzą w zakres niniejszej opinii, ponieważ nie wchodzą w zakres RODO.

Rada stwierdziła, że kilka organów nadzorczych włączyło do swoich wykazów rodzaje przetwarzania, które zasadniczo są przetwarzaniem lokalnym. Biorąc pod uwagę fakt, że art. 35 ust. 6 dotyczy jedynie przetwarzania transgranicznego i przetwarzania, które może mieć wpływ na swobodny przepływ danych osobowych i na osoby, których dane dotyczą, Rada nie przedstawi opinii na temat przetwarzania lokalnego.

Opinia ma na celu określenie spójnego zbioru operacji przetwarzania, które powtarzają się w wykazach przekazanych przez organy nadzorcze.

Oznacza to, że w przypadku ograniczonej liczby rodzajów operacji przetwarzania, które zostaną określone w zharmonizowany sposób, wszystkie organy nadzorcze będą wymagały

dokonania oceny skutków dla ochrony danych, a Rada zaleci tym organom wprowadzenie odpowiednich zmian w swoich wykazach w celu zapewnienia spójności.

Jeżeli w niniejszej opinii nie ma mowy o pozycjach zawartych w przedłożonym wykazie, oznacza to, że Rada nie zwraca się do polskiego organu nadzorczego o podejmowanie dalszych działań.

Rada przypomina ponadto, że kluczowe znaczenie dla administratorów danych i podmiotów przetwarzających dane ma przejrzystość. Rada jest zdania, że – w celu doprecyzowania pozycji w wykazie – zawarcie w wykazie wyraźnych odniesień, w przypadku każdego rodzaju przetwarzania, do kryteriów określonych w wytycznych może przyczynić się do zwiększenia przejrzystości. W związku z tym Rada uważa, że można by dodać wyjaśnienie, które kryteria zostały uwzględnione przez polski organ nadzorczy podczas tworzenia wykazu.

2.2 Zastosowanie mechanizmu spójności do projektu wykazu

Projekt wykazu przedłożony przez polski organ nadzorczy odnosi się do oferowania towarów lub usług osobom, których dane dotyczą, odnosi się do monitorowania zachowania tych osób w kilku państwach członkowskich lub może znacznie wpływać na swobodny przepływ danych osobowych w Unii głównie dlatego, że operacje przetwarzania zawarte w przedłożonym projekcie wykazu nie ograniczają się do osób, których dane dotyczą, w tym państwie.

2.3 Analiza projektu wykazu

Biorąc pod uwagę, że:

a. art. 35 ust. 1 RODO 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. 35 ust. 3 RODO zawiera niewyczerpujący wykaz rodzajów przetwarzania, które wymagają oceny skutków dla ochrony danych;

Rada jest zdania, że:

Orientacyjny charakter wykazu

Jako że w wykazie przedstawionym przez polski organ nadzorczy nie zaznaczono wyraźnie, że wykaz nie jest wyczerpujący, Rada zwraca się o dodanie tego wyjaśnienia do dokumentu zawierającego wykaz.

Odniesienie do wytycznych

Rada jest zdania, że analiza przeprowadzona w wytycznych Grupy Roboczej Art. 29 nr WP 248 stanowi kluczowy element zapewnienia spójności w całej Unii. W związku z tym Rada zwraca się do organów nadzorczych, aby do dokumentów zawierających ich wykazy dodały oświadczenie, że dany wykaz opiera się na tych wytycznych, uzupełnia je i doprecyzowuje.

Jako że dokument polskiego organu nadzorczego nie zawiera takiego oświadczenia, Rada zaleca polskiemu organowi nadzorczemu wprowadzenie w dokumencie odpowiedniej zmiany.

Dane biometryczne

Zgodnie z wykazem przedłożonym przez polski organ nadzorczy w celu uzyskania opinii Rady w przypadku przetwarzania danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej dokonanie oceny skutków dla ochrony danych nie jest obecnie wymagane. W związku z tym Rada zwraca się do polskiego organu nadzorczego o odpowiednią zmianę wykazu poprzez wyraźne dodanie przetwarzania danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej w połączeniu z co najmniej jednym innym kryterium; zmiana ta nie narusza art. 35 ust. 3 RODO.

Dane genetyczne

Zgodnie z wykazem przedłożonym przez polski organ nadzorczy w celu uzyskania opinii Rady w przypadku przetwarzania danych genetycznych dokonanie oceny skutków dla ochrony danych nie jest obecnie wymagane. Rada jest zdania, że przetwarzanie danych genetycznych samo w sobie nie musi stanowić wysokiego ryzyka. Przetwarzanie danych genetycznych w połączeniu z co najmniej jednym innym kryterium wymaga jednak dokonania oceny skutków dla ochrony danych. W związku z tym Rada zwraca się do polskiego organu nadzorczego o odpowiednią zmianę wykazu poprzez wyraźne dodanie przetwarzania danych genetycznych w połączeniu z co najmniej jednym innym kryterium; zmiana ta nie narusza art. 35 ust. 3 RODO.

Dane dotyczące lokalizacji

Rada jest zdania, że spójność jest jedną z podstawowych zasad RODO. Rada zauważyła, że większość przedstawionych wykazów zawiera wyraźne odniesienia do przetwarzania danych dotyczących lokalizacji. Ponieważ wykaz przedstawiony przez polski organ nadzorczy w celu uzyskania opinii nie zawiera takiego odniesienia, Rada zachęca polski organ nadzorczy do uwzględnienia w swoim wykazie przetwarzania danych dotyczących lokalizacji wraz z innym kryterium.

Monitorowanie pracowników

Rada jest zdania, że, ze względu na swój specyficzny charakter, przetwarzanie danych w związku z monitorowaniem pracowników – które to przetwarzanie zgodnie z wytycznymi spełnia kryterium systematycznego monitorowania, a pracownicy spełniają kryterium osób, których dane dotyczą, wymagających szczególnej ochrony – może wymagać dokonania oceny skutków dla ochrony danych. Biorąc pod uwagę fakt, że wykaz przedłożony przez polski organ nadzorczy w celu uzyskania opinii Rady już przewiduje, że tego rodzaju przetwarzanie wymaga dokonania oceny skutków dla ochrony danych, Rada zaleca jedynie podanie wyraźnego odniesienia do tych dwóch kryteriów w wytycznych Grupy Roboczej Art. 29 nr WP 248. Rada jest ponadto zdania, że wytyczne Grupy Roboczej Art. 29 nr WP 249 obowiązują przy definiowaniu pojęcia systematycznego przetwarzania danych osobowych pracowników.

Brak spójności z wytycznymi

Rada zauważyła, że polski organ nadzorczy powtarza kryteria zawarte w wytycznych Grupy Roboczej Art. 29 w pozycjach 2, 4, 5, 6, 8 i 9. W wytycznych stwierdzono jednak, że w większości przypadków administrator danych może uznać, że przetwarzanie danych

spełniające dwa kryteria wymagałoby dokonania oceny skutków dla ochrony danych. W związku z tym Rada jest zdania, że wykaz przedłożony przez polski organ nadzorczy jest niezgodny z wytycznymi. Rada zwraca się zatem do polskiego organu nadzorczego o dostosowanie wykazu do wytycznych poprzez dodanie, że w większości przypadków w odniesieniu do wyżej wymienionych punktów tylko przetwarzanie, które spełnia dwa kryteria, wymagałoby dokonania oceny skutków dla ochrony danych oraz że im więcej kryteriów dane przetwarzanie spełnia, tym większe jest prawdopodobieństwo, że będzie ono stanowiło wysokie ryzyko dla praw i wolności osób, których dane dotyczą, a zatem że konieczne będzie dokonanie oceny skutków dla ochrony danych, niezależnie od środków, które administrator zamierza przyjąć.

Przetwarzanie przy użyciu nowych/innowacyjnych technologii

W wykazie przedstawionym przez polski organ nadzorczy w celu uzyskania opinii Rady przewidziano, że przetwarzanie danych osobowych przy użyciu innowacyjnych technologii, w połączeniu z co najmniej jednym innym kryterium, wymaga dokonania oceny skutków dla ochrony danych. Rada przyjmuje do wiadomości włączenie tego kryterium do wykazu.

3. Wnioski i zalecenia

Projekt wykazu sporządzony przez polski organ nadzorczy może prowadzić do niespójnego stosowania wymogu dokonania oceny skutków dla ochrony danych. W projekcie należy w związku z tym wprowadzić następujące zmiany:

- jeżeli chodzi o orientacyjny charakter wykazu: Rada zwraca się o dodanie wyjaśnienia do dokumentu zawierającego wykaz, aby wskazać na jego niewyczerpujący charakter;
- jeżeli chodzi o odniesienia do wytycznych: Rada zwraca się do polskiego organu nadzorczego o wprowadzenie odpowiednich zmian w dokumencie;
- jeżeli chodzi o dane biometryczne: Rada zwraca się do polskiego organu nadzorczego o odpowiednią zmianę wykazu poprzez wyraźne dodanie przetwarzania danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej w połączeniu z co najmniej jednym innym kryterium;
- jeżeli chodzi o dane genetyczne: Rada zwraca się do polskiego organu nadzorczego o zmianę wykazu poprzez wyraźne dodanie przetwarzania danych genetycznych w połączeniu z co najmniej jednym innym kryterium;
- jeżeli chodzi o dane dotyczące lokalizacji: Rada zachęca polski organ nadzorczy do uwzględnienia w swoim wykazie przetwarzania danych dotyczących lokalizacji wraz z innym kryterium;
- jeżeli chodzi o monitorowanie pracowników: Rada zaleca jedynie dodanie wyraźnego odniesienia do dwóch kryteriów w wytycznych Grupy Roboczej Art. 29 nr WP 248;
- jeżeli chodzi o brak zgodności z wytycznymi: Rada zwraca się do polskiego organu nadzorczego o dostosowanie wykazu do wytycznych poprzez dodanie, że w większości przypadków w odniesieniu do wyżej wymienionych punktów tylko przetwarzanie spełniające dwa kryteria wymagałoby dokonania oceny skutków dla ochrony danych.

4. Uwagi końcowe

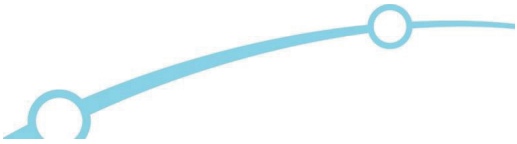
Niniejsza opinia skierowana jest do Urzędu Ochrony Danych Osobowych (polski organ nadzorczy) i zostanie podana do wiadomości publicznej zgodnie z art. 64 ust. 5 lit. b) RODO.

Zgodnie z art. 64 ust. 7 i 8 RODO organ nadzorczy w terminie dwóch tygodni po otrzymaniu niniejszej opinii informuje drogą elektroniczną przewodniczącego EROD, czy podtrzymuje projekt decyzji, czy też go zmieni. W tym samym terminie przekazuje zmieniony projekt wykazu lub – jeżeli nie zamierza kierować się opinią Rady – podaje odpowiednie uzasadnienie, dlaczego nie zamierza się zastosować do całości lub części niniejszej opinii.

W imieniu Europejskiej Rady Ochrony Danych

Przewodnicząca

(Andrea Jelinek)



Opinion 31/2020 on the draft decision of the competent supervisory authority of Poland regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to article 41 GDPR

Adopted on 07 December 2020

Table of contents

The European Data Protection Board

Having regard to Article 63, Article 64 (1)(c), (3)-(8) and Article 41 (3) 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 Article 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 when a supervisory authority (hereinafter "SA") intends to approve the requirements for accreditation of a code of conduct (hereinafter "code") monitoring body pursuant to article 41. The aim of this opinion is therefore to contribute to a harmonised approach with regard to the suggested requirements that a data protection supervisory authority shall draft and that apply during the accreditation of a code monitoring body by the competent supervisory authority. Even though the GDPR does not directly impose a single set of requirements for accreditation, it does promote consistency. The Board seeks to achieve this objective in its opinion by: firstly, requesting the competent SAs to draft their requirements for accreditation of monitoring bodies based on article 41(2) GDPR and on the Board's "Guidelines 1/2019 on Codes of Conduct and Monitoring bodies under Regulation 2016/679" (hereinafter the "Guidelines"), using the eight requirements as outlined in the guidelines' accreditation section (section 12); secondly, providing the competent SAs with written guidance explaining the accreditation requirements; and, finally, requesting the competent SAs to adopt the requirements in line with this opinion, so as to achieve an harmonised approach.

(2) With reference to article 41 GDPR, the competent supervisory authorities shall adopt requirements for accreditation of monitoring bodies of approved codes. They shall, however, apply the consistency mechanism in order to allow the setting of suitable requirements ensuring that monitoring bodies carry out the monitoring of compliance with codes in a competent, consistent and independent manner, thereby facilitating the proper implementation of codes across the Union and, as a result, contributing to the proper application of the GDPR.

(3) In order for a code covering non-public authorities and bodies to be approved, a monitoring body (or bodies) must be identified as part of the code and accredited by the competent SA as being capable of effectively monitoring the code. The GDPR does not define the term "accreditation". However, article 41 (2) of the GDPR outlines general requirements for the accreditation of the monitoring body. There are a number of requirements, which should be met in order to satisfy the competent supervisory authority to accredit a monitoring body. Code owners are required to explain and

[1] References to the "Union" made throughout this opinion should be understood as references to "EEA".

demonstrate how their proposed monitoring body meets the requirements set out in article 41 (2) GDPR to obtain accreditation.

(4) While the requirements for accreditation of monitoring bodies are subject to the consistency mechanism, the development of the accreditation requirements foreseen in the Guidelines should take into consideration the code's sector or specificities. Competent supervisory authorities have discretion with regard to the scope and specificities of each code, and should take into account their relevant legislation. The aim of the Board's opinion is therefore to avoid significant inconsistencies that may affect the performance of monitoring bodies and consequently the reputation of GDPR codes of conduct and their monitoring bodies.

(5) In this respect, the Guidelines adopted by the Board will serve as a guiding thread in the context of the consistency mechanism. Notably, in the Guidelines, the Board has clarified that even though the accreditation of a monitoring body applies only for a specific code, a monitoring body may be accredited for more than one code, provided it satisfies the requirements for accreditation for each code.

(6) 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. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. The Polish Supervisory Authority (hereinafter "PL SA") has submitted its draft decision containing the accreditation requirements for a code of conduct monitoring body to the Board, requesting its opinion pursuant to article 64 (1)(c), for a consistent approach at Union level. The decision on the completeness of the file was taken on 9 October 2020.

2 ASSESSMENT

2.1 General reasoning of the Board regarding the submitted draft accreditation requirements

2. All accreditation requirements submitted to the Board for an opinion must fully address article 41 (2) GDPR criteria and should be in line with the eight areas outlined by the Board in the accreditation section of the Guidelines (section 12, pages 21-25). The Board opinion aims at ensuring consistency and a correct application of article 41 (2) GDPR as regards the presented draft.

3. This means that, when drafting the requirements for the accreditation of a body for monitoring codes according to articles 41 (3) and 57 (1) (p) GDPR, all the SAs should cover these basic core requirements foreseen in the Guidelines, and the Board may recommend that the SAs amend their drafts accordingly to ensure consistency.

4. All codes covering non-public authorities and bodies are required to have accredited monitoring bodies. The GDPR expressly request SAs, the Board and the Commission to "encourage the drawing up of codes of conduct intended to contribute to the proper application of the GDPR, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium sized enterprises." (article 40 (1) GDPR). Therefore, the Board recognises that the requirements need to work for different types of codes, applying to sectors of diverse size, addressing various interests at stake and covering processing activities with different levels of risk.

5. In some areas, the Board will support the development of harmonised requirements by encouraging the SA to consider the examples provided for clarification purposes.

6. When this opinion remains silent on a specific requirement, it means that the Board is not asking the PL SA to take further action.

7. This opinion does not reflect upon items submitted by the PL SA, which are outside the scope of article 41 (2) GDPR, such as references to national legislation. The Board nevertheless notes that national legislation should be in line with the GDPR, where required.

2.2 Analysis of the PL SA's accreditation requirements for Code of Conduct's monitoring bodies

8. Taking into account that:

   a. Article 41 (2) GDPR provides a list of accreditation areas that a monitoring body need to address in order to be accredited;
   b. Article 41 (4) GDPR requires that all codes (excluding those covering public authorities per Article 41 (6)) have an accredited monitoring body; and
   c. Article 57 (1) (p) & (q) GDPR provides that a competent supervisory authority must draft and publish the accreditation requirements for monitoring bodies and conduct the accreditation of a body for monitoring codes of conduct.

   the Board is of the opinion that:

2.2.1 GENERAL REMARKS

9. The Board would like to underline that the obligation of the monitoring body to demonstrate compliance with the accreditation requirements is not limited to the moment it applies for accreditation, but it is an ongoing obligation. In other words, the monitoring body should be able to demonstrate compliance with the requirements at all times.

10. With regard to § 1, section 6.3 of the PL SA's draft accreditation requirements, the Board notes that the reference to the periodic review does not mention that the SA will review the compliance with the requirements periodically. Thus, the Board encourages the PL SA to clarify that the requirements may be reviewed periodically and to provide transparent information on how the periodic review will work in practice and what happens after the expiry of the validity of the accreditation.

11. The Board notes that the requirements include a section on definitions. In this respect, the Board encourages the PL SA to use consistency wording when referring to monitoring body personnel, in

order to avoid confusion. Thus, references to "staff" should be avoided and the correct term should be used when referring to the monitoring body personnel. The Board encourages the PL SA to make the necessary changes (e.g. in sections 2.2, 2.6 under § 3) in order to refer to the monitoring body personnel in a consistent manner.

12. In addition, the Board encourages the PL SA to revise the requirements in order to avoid misunderstandings stemming from the translation of the document into English (for example, "accreditation criteria" should be replaced by "accreditation requirements"; section 4.1.3.3 under § 3 should refer to audit of the member/candidate, instead or "from"; last sentence of section 5.11 under § 3 should read "for example by asking him to confirm it", instead of "to do so"; the reference under section 5.12 under § 3 to "an amicable settlement procedure established by it" should be replaced by "[...] established by the monitoring body"; the reference to the monitoring body's "seat" in section 8.1 under § 3 should be replaced by "establishment" and the reference to the "sharing of responsibility" in section 8.3 under § 3 should be replaced by "bearing of responsibility", as the Board understands it is a translation mistake).

2.2.2 INDEPENDENCE

13. With regard to the specific requirements for accreditation of the monitoring body (under § 3 of the PL SA's draft accreditation requirements), the Board considers that the requirements to demonstrate the independence of the monitoring body (section 1 under § 3) would benefit from the inclusion of examples with regard to the four areas where independence has to be demonstrated. For example, organisational independence can be demonstrated with a differentiated payroll, analytical accounting systems with different responsibility centres or any other logical separation that can rise firewalls between the monitoring body and the code owners or code members. As for financial independence, the monitoring body would not be considered financially independent if the rules governing its financial support allow a code member, who is under investigation by the monitoring body, to stop its financial contributions to it, in order to avoid a potential sanction from the monitoring body. The Board encourages the PL SA to provide examples of how the monitoring body can provide such evidence

14. With respect to definition of independence, the Board encourages the PL SA to elaborate what independence means. To ensure consistency such clarification could rely on the wording agreed by the Board in the previous opinions. According to the Board, independence for a monitoring body should be understood as a series of formal rules and procedures for the appointment, terms of reference and operation of the monitoring body. In Board's view these rules and procedures will allow the monitoring body to perform the monitoring of compliance with a code of conduct in complete autonomy, without being directly or indirectly influenced, nor subject to any form of pressure that might affect its decisions. This means that a monitoring body should not be in a position to receive any instructions regarding the exercise of its task from code members, the profession, industry or sector to which the code applies, or from the code owner itself.

15. The Board observes that the draft accreditation requirements do not make an explicit reference to "accountability" as one of the four areas in which the monitoring body shall demonstrate independence. The Board considers that the independence of the monitoring body shall be demonstrated in four areas: 1) Legal and decision making procedures, 2) financial, 3) organisational

and 4) accountability.[2] Therefore, the Board recommends that the PL SA to include the explicit obligation to demonstrate independence in relation to the accountability of the monitoring body.

16. With regard to the first paragraph of section 1 under § 3 of the PL SA's draft accreditation requirements ("Independence"), the Board considers that the impartiality of the monitoring body from the code members, the profession, industry or sector to which the code applies should be further specified, particularly with regard to any legal and economic links that may exist between the monitoring body and the code owner or code members. In addition, the impartiality must be demonstrated also in relation to the profession or sector. For this reason, the Board encourages the PL SA to amend this paragraph accordingly. In addition, the Board considers that other references to the industry (for example, in sections 3 and 7 under § 3), should be completed in the same line, in order to avoid confusion.

17. With regard to internal monitoring bodies, subsection 1.1.2 under § 3 of the PL SA's draft accreditation requirements refer to the independence of the internal monitoring body in relation to the code owner. The Board recognised the importance of ensuring the impartiality of internal monitoring bodies from the code owner. However, the independence shall also be ensured with regard to code members. Thus, the Board recommends the PL SA to include a reference to the code members as well.

18. With regard to section 1.2 under § 3, the Board considers that the requirements concerning the financial independence should address the boundary conditions that determine the concrete requirements for financial independence and sufficient resources. These include the number, size and complexity of the code members (as monitored entities), the nature and scope of their activities (which are the subject of the code) and the risk(s) associated with the processing operation(s).Therefore, the Board encourages the PL SA to redraft the requirements accordingly.

19. With regard to the example given on subsection 1.2.1 under § 3 as to the source of funding, the Board underlines that in any case, the independence of the monitoring body cannot be in any way compromised. For instance, the monitoring body would not be considered to be financially independent if the rules governing its financial support allow a code member, who is under investigation by the monitoring body, to stop its financial contributions to it, in order to avoid a potential sanction from the monitoring body. The Board encourages the PL SA to add such clarification and examples. In addition, the Board notes that subsection 1.2.1 under § 3 refers to the fees and contributions paid by the code members' candidates. The Board encourages the PL SA to clarify the reference to the code members' candidates.

20. With regard to subsection 1.2.3 under § 3 of the PL SA's draft accreditation requirements, the Board understands that it refers to the long-term financial stability of the monitoring body. However, the Board considers it could be better clarified, to ensure that the monitoring body has procedures in place to ensure its long-term financial stability and that the loss of one or more funding sources does not affect independence. Therefore, the Board encourages the PL SA to include such clarification.

21. With regard to the organisational independence (section 1.3 and in particular, subsection 1.3.2 under § 3), the Board encourages the PL SA to clarify that "material resources" also include technical resources.

[2] The EDPB developed these areas in more detail in the Opinion 9/2019 on the Austrian SA draft accreditation requirements for a code of conduct monitoring body pursuant to article 41 GDPR

22. Regarding subsection 1.3.4 under § 3, the Board notes that the allocation of resources will depend, inter alia, on the "number of code members". Since the number of code members may not be known at the moment the monitoring body applies for accreditation, the Board encourages the PL SA to refer to the expected number and size of the code members.

23. With regard to subsection 1.3.6 under § 3, the Board notes that the obligation of the monitoring body to demonstrate independence is only "during the decision-making process". The Board considers that the independence of the monitoring body is an ongoing process and must be ensured and demonstrated at any time, not only during the decision-making process. In addition, the Board underlines that, in order to demonstrate organisational independence, the monitoring body personnel shall be able to act independently from the code owner and the code members and without being subject to any pressure or influence. Finally, the Board welcomes the inclusion of the example in subsection 1.3.6 under § 3. However, in order to avoid confusion, the example should clearly indicate that it is related to the selection procedure and that the independence of the monitoring body personnel is not limited to the selection procedure, as reflected in the examples provided in par. 13 of this Opinion. Therefore, the Board recommends the PL SA to amend the draft requirements in order to reflect the abovementioned changes.

2.2.3 CONFLICT OF INTEREST

24. As a general remark in this section, the Board is of the opinion that, for practical reasons, examples of cases where a conflict of interest could arise might be helpful. An example of a conflict of interest situation would be the case where personnel conducting audits or making decisions on behalf of a monitoring body had previously worked for the code owner, or for any of the organisations adhering to the code. Therefore, the Board encourages the PL SA to add some examples, similar to the one provided in this paragraph.

25. Furthermore, the Board observes that the PL SA's draft accreditation requirements do not explicitly include the obligation of the monitoring body to refrain from any action that is incompatible with its tasks and duties and to not seek nor take instructions from any person, organisation or association (paragraph 68, page 23 of the Guidelines).Therefore, the Board recommends the PL SA to align the text with the Guidelines by including the above-mentioned obligations.

2.2.4 EXPERTISE

26. Regarding the accreditation requirement in terms of the expertise of the monitoring body (section 3 of the PL SA's draft accreditation requirements), the Board acknowledges that the guidelines set a high bar requiring monitoring bodies to have an in-depth understanding of data protection issues. In addition, the guidelines also require an expert knowledge of the specific processing activities which are the subject matter of the code. The Board acknowledges that section 3.3 under § 3 of the PL SA's draft accreditation requirements address the level of expertise and encourages the PL SA to amend it in order to align the requirements with the guidelines.

27. With regard to section 3.1 under § 3 of the PL SA's draft accreditation requirements, the Board notes that the requirement implies that specific expertise requirements will be laid down in the Code. Whereas the Board welcomes the drafting of codes that include specific expertise requirements, it is also aware that it may not always be the case. Thus, in order to reflect that, the Board encourages the PL SA to replace "will" by "may".

2.2.5 ESTABLISHED PROCEDURES AND STRUCTURES

28. With regard to subsection 4.1.3.2 under § 3, the Board notes that the audit methodology will take into account the "number of code members". Since the number of code members may not be known at the moment the monitoring body applies for accreditation, the Board encourages the PL SA to refer to the expected number and size of the code members and the complaints received.

2.2.6 TRANSPARENT COMPLAINT HANDLING

29. Regarding subsection 5.4.3 under § 3 of the PL SA's draft accreditation requirements, the Board acknowledges that the complaints handling procedure shall include, at least, "time limits for dealing with the complaint". The Board is of the opinion that further clarification is needed with regard to the time limits for dealing with complaints. In this regard, the procedure should envisage that the monitoring body has to inform the complainant with progress reports or the outcome of the complaint, within a reasonable time frame (e.g. 3 months). This period could be extended when necessary, taking into account the size of the organisation under investigation, as well as the size of the investigation. Therefore, the Board recommends that the PL SA redraft the requirement accordingly.

30. With regard to section 5.7 under § 3 of the PL SA's draft accreditation requirements, the Board encourages the PL SA to redraft it as an actual requirements (i.e. starting with "the monitoring body shall...").

31. Section 5.8 under § 3 of the PL SA's draft accreditation requirements establishes the obligation of the monitoring body to inform the SA "of the actions taken in respect of complaints submitted". The Board notes that the information obligation is also towards the code member, the code owner and all concerned SAs, as stated in the Guidelines (par. 77). Therefore, the Board recommends that the PL SA amend the requirement accordingly.

2.2.7 COMMUNICATION WITH THE PL SA

32. Section 6.1 under § 3 of the PL SA's draft accreditation requirements establishes the obligation of the monitoring body to submit an annual report to the SA on all its activities in relation to the Code of Conduct. The following sections also develop situations in which the monitoring body will communicate with the PL SA. In addition, subsection 4.1.3.8 establishes regular reporting obligations of the monitoring body. The Board considers that the information on the functioning of the monitoring body activities (for example, actions taken by the MB) should also be available to the PL SA on its request, and encourages the PL SA to include such reference.

33. In addition, the Board encourages the PL SA to make the link between subsection 6.2.6 under § 3 and subsection 6.2.8 under § 3 clearer, in order to avoid misunderstandings with regard to the type of audits.

34. Regarding section 6.3 under § 3, the Board notes that the example given would only be relevant in case the code of conduct covers the obligations under article 33 GDPR. Therefore, the Board encourages the PL SA to clarify this in the example.

35. Regarding section 6.5 under § 3, the Board notes that the accreditation requirements state that significant changes "may result in a review of the accreditation". The Board is of the opinion that, when a substantial change has been performed, the review of the accreditation is not merely a possibility, but rather an obligation. Therefore, the Board recommends the PL SA to rephrase the wording, by stating that substantial changes would result in a review of the accreditation.

2.2.8 REVIEW MECHANISMS

36. Section 7.1 under § 3 of the PL SA's draft accreditation requirements establishes the obligation of the monitoring body to provide a procedure to assist with the periodic review of the code of conduct. The Board is of the opinion that the monitoring body also has a key role in applying code updates (amendments of extensions of the code) following the instructions of the code owner, and encourages the PL SA to include such reference. In addition, the Board considers that the reference to section 4.1.3 under § 3 should be replaced by 4.1.4 under § 3 and that a reference to section 6.2.5 under § 3 would be helpful, as an example of the elements to be considered, and encourages the PL SA to amend the draft accordingly.

37. With regard to section 7.5 under § 3, the Board notes the reporting is only to the code owner. The Board encourages accreditation requirements which require a monitoring body to develop mechanisms that enable feedback to the code owners and to any other entity referred to in the code of conduct. Therefore, the Board encourages the PL SA to include the abovementioned reference in the draft requirements.

38. In addition, the Board considers that the information related to the review carried out should be at the disposal of the SA, and encourages the PL SA to amend the draft accordingly.

2.2.9 LEGAL STATUS

39. With regard to section 8.3 under § 3, the Board underlines that the monitoring body should have financial and other resources, and the necessary procedures to ensure the monitoring body activity. Thereby, the Board encourages that the PL SA specify that the monitoring body shall have adequate financial and other resources and the necessary procedures to ensure its functioning.

40. Moreover, the code of conduct itself will need to demonstrate that the operation of the code's monitoring mechanism is sustainable over time, covering worst-case scenarios, such as the monitoring body being unable to perform the monitoring function. In this regard, it would be advisable to require that a monitoring body demonstrates that it can deliver the code of conduct's monitoring mechanism over a suitable period of time. Therefore, the Board recommends PL SA to explicitly require that monitoring bodies demonstrate continuity of the monitoring function over time.

41. The Board observes that, according to subsection 8.7.1 under § 3 of the PL SA's draft accreditation requirements, when using sub-contractors for processes relating to monitoring actions, evidence for demonstrating the compliance of the subcontractor with the requirements may include "a contract setting out the responsibilities and responsibilities of the parties, confidentiality, the categories of personal data processed and the obligation to provide adequate security for them". The Board encourages the PL SA to redraft the text in order to include requirements relating to the termination of those contracts, in particular so as to ensure that the subcontractors fulfil their data protection obligations.

42. The Board notes that section 8.9 under § 3 states that "the use of subcontracting does not exempt the monitoring body from the responsibility of the monitoring body under the GDPR". The Board is of the opinion that, even when subcontractors are used, the monitoring body shall ensure effective monitoring of the services provided by the contracting entity. Although the Board realises that section 8.9 under § 3 seems to imply that, the Board recommends the PL SA to explicitly clarify it. In addition, the monitoring body should be the ultimate responsible for all the decisions taken related to its monitoring function. Therefore, the Board encourages the PL SA to specify that, notwithstanding the

sub-contractor's responsibility and obligations, the monitoring body is always the ultimate responsible for the decision-making and for compliance.

3 CONCLUSIONS / RECOMMENDATIONS

43. The draft accreditation requirements of the Polish Supervisory Authority may lead to an inconsistent application of the accreditation of monitoring bodies and the following changes need to be made:

44. Regarding *independence* the Board recommends that the PL SA:

    1. include the explicit obligation to demonstrate independence in relation to the accountability of the monitoring body.
    2. include a reference to code members with regard to the independence of internal monitoring bodies in subsection 1.1.2 under § 3.
    3. amend subsection 1.3.6 under § 3 in order to reflect the remarks made in paragraph 23 of this Opinion

45. Regarding *conflict of interest* the Board recommends that the PL SA:

    1. explicitly include the obligation of the monitoring body to refrain from any action that is incompatible with its tasks and duties and to not seek nor take instructions from any person, organisation or association

46. Regarding *transparent complaint handling* the Board recommends that the PL SA:

    1. redraft subsection 5.4.3 under § 3 in order to take into account that the monitoring body has to inform the complainant with progress reports or the outcome of the complaint, within a reasonable time frame (e.g. 3 months). This period could be extended when necessary.
    2. include, among the addressees of the information referred to in section 5.8 under § 3, the code member, the code owner and all concerned SAs.

47. Regarding *communication with the PL SA* the Board recommends that the PL SA:

    1. rephrase the wording in section 6.5 under § 3, by stating that substantial changes would result in a review of the accreditation.

48. Regarding *legal status* the Board recommends that the PL SA:

    1. amend the requirements in order to explicitly require that monitoring bodies demonstrate continuity of the monitoring function over time.
    2. clarify, section 8.9 under § 3, that even when subcontractors are used, the monitoring body shall ensure effective monitoring of the services provided by the contracting entity

4 FINAL REMARKS

49. This opinion is addressed to the Polish supervisory authority and will be made public pursuant to Article 64 (5) (b) GDPR.

50. According to Article 64 (7) and (8) GDPR, the PL SA shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft decision. Within the same period, it shall provide the amended draft decision or where it does not intend to follow the opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this opinion, in whole or in part.

51. The PL SA 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)

KOMISJA
EUROPEJSKA

Bruksela, dnia 24.1.2018r.
COM(2018) 43 final

KOMUNIKAT KOMISJI DO PARLAMENTU EUROPEJSKIEGO I RADY

Wzmocniona ochrona, nowe możliwości – wytyczne Komisji dotyczące bezpośredniego stosowania ogólnego rozporządzenia o ochronie danych od dnia 25 maja 2018 r.

Komunikat Komisji do Parlamentu Europejskiego i Rady

Wzmocniona ochrona, nowe możliwości – wytyczne Komisji dotyczące bezpośredniego stosowania ogólnego rozporządzenia o ochronie danych od dnia 25 maja 2018 r.

Wprowadzenie

W dniu 6 kwietnia 2016 r. UE wyraziła zgodę na przeprowadzenie ważnej reformy swoich ram ochrony danych, polegającej na przyjęciu pakietu dotyczącego reformy ochrony danych, w którego skład wchodzi ogólne rozporządzenie o ochronie danych (RODO)[1], zastępujące obowiązującą od dwudziestu lat dyrektywę 95/46/WE[2] („dyrektywa o ochronie danych"), i dyrektywa w sprawie policji[3]. Dnia 25 maja 2018 r., dwa lata po przyjęciu i wejściu w życie, rozpocznie się bezpośrednie stosowanie nowego, obejmującego swoim zasięgiem całą UE instrumentu ochrony danych – ogólnego rozporządzenia o ochronie danych („rozporządzenie")[4].

Nowe rozporządzenie wzmocni ochronę prawa osób fizycznych do ochrony danych osobowych, odzwierciedlając fakt, że ochrona danych stanowi prawo podstawowe Unii Europejskiej[5].

Zapewniając jeden zestaw przepisów mających bezpośrednie zastosowanie w porządku prawnym państw członkowskich, rozporządzenie zagwarantuje swobodny przepływ danych osobowych między państwami członkowskimi UE oraz wzmocni dwa nieodzowne elementy jednolitego rynku cyfrowego: zaufanie konsumentów i ich bezpieczeństwo. W ten sposób rozporządzenie wprowadzi nowe możliwości dla firm i przedsiębiorstw, szczególnie tych mniejszych, również za sprawą wyjaśnienia przepisów dotyczących międzynarodowego przekazywania danych.

Nowe ramy ochrony danych bazują wprawdzie na obowiązujących obecnie przepisach prawa, ich wprowadzenie będzie miało jednak daleko idące skutki i będzie wymagało znacznych dostosowań w określonych kwestiach. Z tego względu w rozporządzeniu przewidziano dwuletni okres przejściowy trwający do dnia 25 maja 2018 r., aby państwa członkowskie i zainteresowane strony miały czas w pełni przygotować się do stosowania nowych ram prawnych.

---

[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.

[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, Dz.U. L 281 z 23.11.1995.

[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, Dz.U. L 119 z 4.5.2016.

[4] Rozporządzenie weszło w życie w dniu 24 maja 2016 r. i będzie miało zastosowanie od dnia 25 maja 2018 r.

[5] Prawo to zapisano w art. 8 Karty praw podstawowych Unii Europejskiej i w art. 16 TFUE.

Przez ostatnie dwa lata wszystkie zainteresowane strony, od administracji krajowych i krajowych organów ochrony danych, aż po administratorów i podmioty przetwarzające, uczestniczyły w licznych działaniach, zapewniając, aby znaczenie i skala zmian wiążących się z nowymi przepisami o ochronie danych zostały dobrze zrozumiane, a wszystkie podmioty były gotowe do stosowania tych przepisów. W związku z tym, że do dnia 25 maja pozostało już mało czasu, Komisja jest zdania, że należy ocenić przeprowadzone prace i rozważyć wszelkie kolejne działania, które warto przeprowadzić w celu zapewnienia, aby wprowadzone zostały wszystkie elementy konieczne do skutecznego wejścia w życie nowych ram[6].

W niniejszym komunikacie:

- podsumowano najważniejsze innowacje i możliwości stwarzane przez nowe przepisy UE w dziedzinie ochrony danych;
- podsumowano prace przygotowawcze przeprowadzone dotychczas na szczeblu UE;
- przedstawiono dalsze działania, które powinny zostać podjęte przez Komisję Europejską, krajowe organy ochrony danych i krajowe administracje dla skutecznego zakończenia etapu przygotowań;
- określono środki, które Komisja zamierza podjąć w nadchodzących miesiącach.

Ponadto równolegle z przyjęciem niniejszego komunikatu Komisja uruchamia zestaw narzędzi internetowych, aby pomóc zainteresowanym stronom w przygotowaniach do stosowania rozporządzenia, oraz kampanię informacyjną we wszystkich państwach członkowskich, wspieraną przez biura przedstawicielstw.

1. NOWE UNIJNE RAMY OCHRONY DANYCH – WZMOCNIONA OCHRONA I NOWE MOŻLIWOŚCI

Rozporządzenie nadal bazuje wprawdzie na podejściu przyjętym w dyrektywie o ochronie danych, jednak wyjaśniono w nim i zaktualizowano przepisy o ochronie danych w oparciu o 20 lat doświadczeń w zakresie stosowania przepisów UE w dziedzinie ochrony danych i odpowiednie orzecznictwo z tego samego okresu; wprowadzono w nim szereg nowych elementów, które mają na celu wzmocnienie ochrony prawa osób fizycznych i stworzenie nowych możliwości dla firm i przedsiębiorstw. Należą do nich w szczególności:

- **zharmonizowane ramy prawne prowadzące do jednolitego stosowania przepisów z korzyścią dla unijnego jednolitego rynku cyfrowego.** Oznacza to jeden zestaw przepisów dla obywateli i przedsiębiorstw. Jest to odpowiedź na panującą obecnie sytuację, w której państwa członkowskie UE wykonują przepisy dyrektywy w różny sposób. Aby zapewnić jednakowe i spójne stosowanie przepisów we wszystkich państwach członkowskich, wprowadza się mechanizm kompleksowej współpracy;

- **równe warunki działania dla wszystkich przedsiębiorstw prowadzących działalność na rynku UE**. Rozporządzenie zawiera wymóg, aby przedsiębiorstwa z siedzibą poza UE oferujące towary i usługi, z którymi wiąże się przetwarzanie danych osobowych, lub monitorujące zachowanie osób fizycznych w Unii stosowały te same przepisy, które stosują przedsiębiorstwa z siedzibą w UE. Przedsiębiorstwa spoza UE prowadzące działalność na jednolitym rynku muszą w określonych okolicznościach wyznaczyć

[6] https://ec.europa.eu/commission/sites/beta-political/files/letter-of-intent-2017_pl.pdf

przedstawiciela w UE, do którego obywatele i organy mogą zwracać się oprócz lub zamiast do danego przedsiębiorstwa z siedzibą za granicą;

- **zasada uwzględniania ochrony danych w fazie projektowania i zasada domyślnej ochrony danych**, które stwarzają zachęty do przyjmowania innowacyjnych rozwiązań związanych z ochroną danych już w fazie początkowej;

- **wzmocnione prawa osób fizycznych.** W rozporządzeniu wprowadzono: nowe wymogi w zakresie przejrzystości; wzmocnione prawo do informacji, prawo dostępu i prawo do usunięcia danych („prawo do bycia zapomnianym"); zasadę, zgodnie z którą milczenie lub niepodjęcie działania nie będzie już uznawane za ważne wyrażenie zgody, ponieważ dla wyrażenia zgody wymagane będzie wyraźne działanie potwierdzające; ochronę dzieci w internecie;

- **większa kontrola sprawowana przez osoby fizyczne nad ich danymi osobowymi.** W rozporządzeniu ustanowiono **nowe prawo do przenoszenia danych** umożliwiające obywatelom zażądanie od przedsiębiorstwa lub organizacji, aby przesłały z powrotem dane osobowe dostarczone temu przedsiębiorstwu lub tej organizacji przez dane osoby fizyczne za ich własną zgodą lub na podstawie umowy. Na podstawie tego prawa możliwe będzie również bezpośrednie przekazywanie danych innemu przedsiębiorstwu lub innej organizacji, o ile jest to technicznie możliwe. Prawo do przenoszenia danych umożliwia przesłanie danych osobowych przez jedno przedsiębiorstwo lub jedną organizację bezpośrednio innemu przedsiębiorstwu lub innej organizacji, w związku z czym prawo to wesprze również swobodny przepływ danych osobowych w UE, będzie zapobiegać blokadzie danych osobowych i będzie sprzyjać konkurencji między przedsiębiorstwami. Ułatwienie obywatelom zmiany dostawców usług będzie sprzyjać rozwojowi nowych usług w kontekście strategii jednolitego rynku cyfrowego;

- **wzmocniona ochrona przed naruszeniami ochrony danych**. W rozporządzeniu ustanowiono kompleksowy zestaw przepisów dotyczących naruszeń ochrony danych osobowych. Wyraźnie określono w nim, czym jest „naruszenie ochrony danych osobowych", a także wprowadzono obowiązek zgłoszenia naruszenia organowi nadzorczemu nie później niż w terminie 72 godzin po jego stwierdzeniu w sytuacjach, w których dane naruszenie ochrony danych może powodować ryzyko naruszenia praw lub wolności osób fizycznych. W określonych okolicznościach w rozporządzeniu zobowiązano do powiadomienia o naruszeniu osobę fizyczną, której danych dotyczy dane naruszenie. Pozwala to znacznie wzmocnić ochronę w porównaniu z obecną sytuacją w UE, w której jedynie dostawcy usług łączności elektronicznej, operatorzy usług kluczowych i dostawcy usług cyfrowych są obowiązani do zgłaszania naruszeń ochrony danych na podstawie odpowiednio dyrektywy o prywatności i łączności elektronicznej[7] i dyrektywy w sprawie bezpieczeństwa sieci i systemów informatycznych[8];

---

[7] 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. 37–47. Zgodnie z art. 95 ogólnego rozporządzenia o ochronie danych rozporządzenie to nie nakłada dodatkowych obowiązków na osoby fizyczne ani prawne w sprawach, w których podmioty te podlegają szczegółowym obowiązkom mającym ten sam cel określonym w dyrektywie 2002/58/WE. Oznacza to na przykład, że podmioty objęte dyrektywą o prywatności i łączności elektronicznej są objęte przewidzianym w tej dyrektywie obowiązkiem zgłaszania naruszenia danych osobowych w zakresie, w jakim naruszenie dotyczy usługi objętej tą dyrektywą. W tym

- **na mocy rozporządzenia wszystkim organom ochrony danych nadano uprawnienie do nakładania kar pieniężnych na administratorów i podmioty przetwarzające.** Obecnie nie wszystkie organy ochrony danych mają takie uprawnienie. Usprawni to wykonywanie przepisów. Kary pieniężne mogą sięgać kwoty 20 mln EUR lub, w przypadku przedsiębiorstwa – 4 % jego rocznego światowego obrotu;

- **większa elastyczność administratorów i podmiotów przetwarzających dane osobowe za sprawą jednoznacznych przepisów dotyczących odpowiedzialności (zasada rozliczalności).** W rozporządzeniu zdecydowano się odejść od systemu zawiadamiania na rzecz zasady rozliczalności. Zasadę rozliczalności wykonuje się w drodze skalowalnych obowiązków w zależności od ryzyka (np. obecność inspektora ochrony danych lub obowiązek przeprowadzania ocen skutków dla ochrony danych). Wprowadzono nowe narzędzie, które pomoże w przeprowadzeniu oceny ryzyka przed rozpoczęciem przetwarzania danych: ocena skutków dla ochrony danych. Ta ostatnia jest wymagana, gdy przetwarzanie może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych. W rozporządzeniu wyraźnie wymieniono trzy sytuacje, w których zachodzi taka konieczność: gdy przedsiębiorstwo prowadzi systematyczną i kompleksową ocenę czynników osobowych odnoszących się do osób fizycznych (w tym profilowanie), przetwarza na dużą skalę dane wrażliwe lub systematycznie monitoruje na dużą skalę miejsca dostępne publicznie. Krajowe organy ochrony danych będą musiały podawać do publicznej wiadomości wykazy sytuacji podlegających wymogowi dokonania oceny skutków dla ochrony danych[9];

- **większa przejrzystość w zakresie obowiązków podmiotów przetwarzających i odpowiedzialności administratorów w momencie wyboru podmiotu przetwarzającego;**

- **nowoczesny system zarządzania zapewniający bardziej konsekwentne i zdecydowane egzekwowanie przepisów.** Obejmuje to zharmonizowane uprawnienia organów ochrony danych – w tym w zakresie kar pieniężnych – oraz nowe mechanizmy współpracy między tymi organami w ramach sieci;

- **w rozporządzeniu zapewniono utrzymanie wysokiego stopnia ochrony danych osobowych przy ich przekazywaniu poza UE**[10]. Chociaż zasadniczo utrzymano strukturę przepisów dotyczących międzynarodowego przekazywania danych zastosowaną w dyrektywie z 1995 r., to jednak w ramach reformy wyjaśniono i uproszczono ich stosowanie oraz wprowadzono nowe narzędzia w zakresie przekazywania danych. Jeżeli chodzi o decyzje stwierdzające odpowiedni stopień ochrony, w rozporządzeniu

---

zakresie ogólne rozporządzenie o ochronie danych nie nakłada na te podmioty żadnych dodatkowych obowiązków.

[8] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, Dz.U. L 194 z 19.7.2016, s. 1–30. Podmioty objęte zakresem stosowania dyrektywy w sprawie bezpieczeństwa sieci i systemów informatycznych powinny zgłaszać incydenty mające istotny lub znaczny wpływ na świadczenie niektórych ich usług. Zgłaszanie incydentów na podstawie dyrektywy w sprawie bezpieczeństwa sieci i systemów informatycznych pozostaje bez uszczerbku dla zgłaszania naruszeń na podstawie rozporządzenia.

[9] Art. 35 rozporządzenia.

[10] Komunikat Komisji „Wymiana i ochrona danych osobowych w zglobalizowanym świecie", COM(2017) 7 final.

wprowadzono precyzyjny i szczegółowy katalog elementów, które Komisja musi uwzględnić przy ocenie kwestii, czy dany zagraniczny system zapewnia odpowiedni poziom ochrony danych osobowych. W rozporządzeniu formalizuje się również alternatywne instrumenty przekazywania danych, takie jak standardowe klauzule umowne i wiążące reguły korporacyjne, oraz zwiększa ich liczbę.

Dzięki przyjęciu zmienionego rozporządzenia dotyczącego unijnych instytucji, organów i jednostek organizacyjnych[11] i rozporządzenia w sprawie prywatności i łączności elektronicznej[12], które obecnie znajdują się na etapie negocjacji, UE zostanie wyposażona w silny i kompleksowy zestaw przepisów o ochronie danych[13].

2. PRACE PRZYGOTOWAWCZE PRZEPROWADZONE DOTYCHCZAS NA SZCZEBLU UE

Skuteczne stosowanie rozporządzenia wymaga współpracy między wszystkimi podmiotami zaangażowanymi w ochronę danych: państwami członkowskimi, w tym organami administracji publicznej, krajowymi organami ochrony danych, przedsiębiorstwami, organizacjami zajmującymi się przetwarzaniem danych osobowych oraz osobami fizycznymi, a także Komisją.

2.1. Działania podejmowane przez Komisję Europejską

W połowie 2016 r., krótko po wejściu rozporządzenia w życie, Komisja nawiązała dialog z organami państw członkowskich, organami ochrony danych i zainteresowanymi stronami w celu przygotowania ich do stosowania rozporządzenia oraz zapewnienia wsparcia i udzielenia wskazówek.

a) Wspieranie państw członkowskich i ich organów

Komisja bardzo ściśle współpracuje z państwami członkowskimi, aby wesprzeć ich działania podczas okresu przejściowego celem zapewnienia najwyższego możliwego poziomu spójności. W tym celu Komisja utworzyła grupę ekspertów, która ma pomagać państwom członkowskim w ich wysiłkach na rzecz przygotowania się do wejścia rozporządzenia w życie. Grupa ta, która odbyła już 13 spotkań, ma charakter forum, na którym państwa członkowskie mogą dzielić się swoimi doświadczeniami i wiedzą fachową[14]. Komisja zorganizowała również dwustronne spotkania z organami państw członkowskich w celu omówienia kwestii pojawiających się na szczeblu krajowym.

---

[11] Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady dotyczącego ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez unijne instytucje, organy i jednostki organizacyjne oraz swobodnego przepływu takich danych i uchylający rozporządzenie (WE) nr 45/2001 i decyzję nr 1247/2002/WE, COM(2017) 8 final.

[12] Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej i uchylającego dyrektywę 2002/58/WE (rozporządzenie w sprawie prywatności i łączności elektronicznej), COM(2017) 10 final.

[13] Do czasu przyjęcia i wejścia w życie rozporządzenia w sprawie prywatności i łączności elektronicznej dyrektywa 2002/58/WE ma zastosowanie jako *lex specialis* względem rozporządzenia.

[14] Pełen wykaz spotkań, porządki obrad, streszczenia przeprowadzonych dyskusji i przegląd aktualnej sytuacji w zakresie przepisów obowiązujących w różnych państwach członkowskich można znaleźć pod adresem: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3461&Lang=PL

b) Wspieranie poszczególnych organów ochrony danych i utworzenie Europejskiej Rady Ochrony Danych

Komisja aktywnie wspiera prace Grupy Roboczej Art. 29, mając na uwadze również zapewnienie sprawnego przejścia do funkcjonowania Europejskiej Rady Ochrony Danych[15].

c) Działania na arenie międzynarodowej

Rozporządzenie pozwoli jeszcze bardziej wzmocnić zdolność UE do aktywnego propagowania reprezentowanych przez nią wartości w zakresie ochrony danych, a także ułatwić transgraniczne przepływy danych poprzez wspieranie ujednolicania systemów prawnych w skali światowej[16]. Na forum międzynarodowym coraz częściej uznaje się, że unijne przepisy o ochronie danych wyznaczają najwyższe standardy ochrony danych na świecie. Prowadzone są również prace nad unowocześnieniem Konwencji Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, która jest jedynym prawnie wiążącym, wielostronnym instrumentem w obszarze ochrony danych osobowych. Komisja dąży do tego, aby konwencja odzwierciedlała te same zasady, które zapisano w nowych unijnych przepisach o ochronie danych, co przyczyni się do ustanowienia jednolitego zestawu wysokich standardów ochrony danych. Komisja będzie aktywnie wspierać szybkie przyjęcie zaktualizowanego tekstu konwencji ze względu na perspektywę przystąpienia UE do tej konwencji[17]. Komisja zachęca państwa trzecie do ratyfikacji Konwencji Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych i jej protokołu dodatkowego.

Ponadto niektóre kraje i organizacje regionalne spoza UE – począwszy od tych będących w naszym bezpośrednim sąsiedztwie, aż po te, które znajdują się w Azji, Ameryce Łacińskiej i Afryce – przyjmują nowe przepisy w dziedzinie ochrony danych lub aktualizują przepisy już obowiązujące, aby w ten sposób wykorzystać możliwości, jakie daje światowa gospodarka cyfrowa, a także aby odpowiedzieć na rosnące zapotrzebowanie na poprawę bezpieczeństwa danych i ochrony prywatności. Poszczególne państwa różnią się wprawdzie pod względem stosowanego podejścia i stopnia zaawansowania procesu legislacyjnego, można jednak zauważyć oznaki sugerujące, że rozporządzenie w coraz większym stopniu służy za punkt odniesienia i źródło inspiracji[18].

W tym kontekście Komisja prowadzi działania na arenie międzynarodowej zgodnie ze swoim komunikatem ze stycznia 2017 r.[19], aktywnie angażując się we współpracę z kluczowymi partnerami, zwłaszcza w Azji Wschodniej i Południowo-Wschodniej oraz Ameryce

---

[15] Przykładowo Komisja zapewni Europejskiej Radzie Ochrony Danych możliwość wykorzystania systemu wymiany informacji na rynku wewnętrznym (IMI) do komunikacji między jej członkami.

[16] Dokument otwierający debatę w sprawie wykorzystania możliwości płynących z globalizacji, COM(2017) 240.

[17] Konwencja Rady Europy z dnia 28 stycznia 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (ETS nr 108) oraz Protokół dodatkowy z 2001 r. do Konwencji o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych dotyczący organów nadzoru i transgranicznych przepływów danych (ETS nr 181). Do konwencji mogą przystąpić państwa niebędące członkami Rady Europy i ratyfikowało ją już 51 państw (w tym Urugwaj, Mauritius, Senegal i Tunezja).

[18] Zob. np. „Standardy ochrony danych państw iberoamerykańskich", http://www.redipd.es/documentacion/common/Estandares_eng_Con_logo_RIPD.pdf

[19] COM(2017) 7.

Łacińskiej, dążąc do rozpoznania możliwości przyjęcia decyzji stwierdzających odpowiedni stopień ochrony[20].

W szczególności Komisja współpracuje z Japonią w zakresie osiągnięcia celu, jakim jest równoczesne uznanie przez obie strony odpowiedniego stopnia ochrony nie później niż do początku 2018 r., zgodnie z treścią wspólnego oświadczenia przewodniczącego Jeana-Claude'a Junckera i premiera Shinzo Abe z dnia 6 lipca 2017 r.[21]. Rozpoczęto również rozmowy z Republiką Korei dotyczące możliwego przyjęcia decyzji stwierdzającej odpowiedni stopień ochrony. Przyjęcie decyzji stwierdzającej odpowiedni stopień ochrony zapewniłoby swobodny przepływ danych w zainteresowanych państwach trzecich, przy jednoczesnym zagwarantowaniu niezbędnego stopnia ochrony danych osobowych przesyłanych z UE do tych krajów.

Jednocześnie Komisja współpracuje z zainteresowanymi stronami w celu wykorzystania pełnego potencjału zestawu narzędzi oferowanych przez ogólne rozporządzenie o ochronie danych na potrzeby międzynarodowego przekazywania danych, opracowując alternatywne mechanizmy przekazywania danych, które będą dopasowane do szczególnych potrzeb lub sytuacji poszczególnych branż lub podmiotów gospodarczych[22].

d) Współpraca z zainteresowanymi stronami

Komisja zorganizowała szereg wydarzeń mających na celu dotarcie do zainteresowanych stron[23]. Na pierwszy kwartał 2018 r. planowane są nowe warsztaty skierowane do konsumentów. Odbyły się również tematyczne dyskusje sektorowe na temat dziedzin takich jak badania i usługi finansowe.

Komisja utworzyła również grupę różnych zainteresowanych stron ds. rozporządzenia złożoną z przedstawicieli organizacji społeczeństwa obywatelskiego, biznesu, środowisk akademickich i osób zajmujących się przedmiotowymi zagadnieniami od strony praktycznej. Grupa ta będzie doradzać Komisji w szczególności w kwestii sposobów osiągnięcia przez zainteresowane strony odpowiedniego poziomu świadomości w zakresie rozporządzenia[24].

Ponadto Komisja Europejska, za pośrednictwem swojego programu ramowego w zakresie badań naukowych i innowacji „Horyzont 2020"[25], finansuje działania na rzecz opracowywania narzędzi wspierających skuteczne stosowanie przepisów dotyczących wyrażania zgody, które przewidziano w rozporządzeniu, oraz działania dotyczące zapewniających ochronę danych metod analizy danych, takich jak obliczanie wielostronne i szyfrowanie homomorficzne.

2.2. Działania prowadzone przez Grupę Roboczą Art. 29 / Europejską Radę Ochrony Danych

[20] COM(2017) 7, tamże s. 10–11.
[21] http://europa.eu/rapid/press-release_STATEMENT-17-1917_en.htm
[22] COM(2017) 7, tamże s. 10–11.
[23] Dwa warsztaty z udziałem przedstawicieli branży w lipcu 2016 r. i kwietniu 2017 r., dwa wydarzenia polegające na rozmowach przy okrągłym stole na tematy biznesowe w grudniu 2016 r. i maju 2017 r., warsztaty na temat danych dotyczących zdrowia w październiku 2017 r. oraz warsztaty z udziałem przedstawicieli MŚP w listopadzie 2017 r.
[24] http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3537
[25] https://ec.europa.eu/programmes/horizon2020/h2020-sections

Grupa Robocza Art. 29 – w skład której wchodzą wszystkie krajowe organy ochrony danych, w tym Europejski Inspektor Ochrony Danych – odgrywa istotną rolę w przygotowaniu do stosowania rozporządzenia poprzez przygotowywanie wytycznych dla przedsiębiorstw i zainteresowanych stron. Ponieważ krajowe organy ochrony danych egzekwują stosowanie rozporządzenia i stanowią główny punkt kontaktu dla zainteresowanych stron, są one w stanie najlepiej zapewnić większą pewność prawa w kwestii interpretacji rozporządzenia.

Wytyczne / dokumenty robocze przygotowane przez Grupę Roboczą Art. 29 na potrzeby rozpoczęcia stosowania rozporządzenia[26]	
Prawo do przenoszenia danych	Przyjęto w dniach 4–5 kwietnia 2017 r.
Inspektorzy ochrony danych	
Wyznaczenie wiodącego organu nadzorczego	
Ocena skutków dla ochrony danych	Przyjęto w dniach 3–4 października 2017 r.
Administracyjne kary pieniężne	Przyjęto w dniach 3–4 października 2017 r.
Profilowanie	Prace w toku
Naruszenia ochrony danych osobowych	Prace w toku
Zgoda	Prace w toku
Przejrzystość	Prace w toku
Certyfikacja i akredytacja	Prace w toku
Odpowiedni stopień ochrony przekazywanych danych osobowych	Prace w toku
Wiążące reguły korporacyjne dla administratorów danych	Prace w toku
Wiążące reguły korporacyjne dla przetwarzających	Prace w toku

Grupa Robocza Art. 29 pracuje nad aktualizacją istniejących opinii, w tym dotyczących narzędzi przesyłania danych do państw trzecich.

Ponieważ niezbędne jest, aby podmioty gospodarcze miały dostęp do spójnego i jednolitego zestawu wytycznych, obecne wytyczne na szczeblu krajowym muszą zostać albo uchylone, albo dostosowane do przyjętych przez Grupę Roboczą Art. 29 / Europejską Radę Ochrony Danych wytycznych dotyczących tych samych zagadnień.

Komisja przywiązuje szczególną wagę do objęcia wytycznych konsultacjami publicznymi przed finalizacją. Konieczne jest, aby wkład zainteresowanych stron w ten proces był jak najdokładniejszy i jak najkonkretniejszy, co pomoże we wskazaniu najlepszych praktyk i zwróci uwagę Grupy Roboczej Art. 29 na cechy branżowe i sektorowe. Ostateczna

[26] Wszystkie przyjęte wytyczne są dostępne pod adresem: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

odpowiedzialność za te wytyczne spoczywa na Grupie Roboczej Art. 29 i przyszłej Europejskiej Radzie Ochrony Danych, i to do nich organy ochrony danych będą zwracać się podczas egzekwowania rozporządzenia.

Powinna istnieć możliwość zmiany wytycznych ze względu na rozwój sytuacji i stosowane praktyki. W związku z tym ważne jest, aby organy ochrony danych promowały kulturę dialogu ze wszystkimi zainteresowanymi stronami, w tym z przedsiębiorstwami.

Należy pamiętać, że jeżeli pojawią się wątpliwości dotyczące stosowania rozporządzenia, ostateczną interpretację rozporządzenia zapewnią sądy na szczeblach krajowym i unijnym.

3. POZOSTAŁE DZIAŁANIA, KTÓRYCH WYMAGA SKUTECZNE PRZYGOTOWANIE

3.1. Finalizacja ustanawiania ram prawnych na szczeblu krajowym przez państwa członkowskie

Rozporządzenie ma bezpośrednie zastosowanie we wszystkich państwach członkowskich[27]. Oznacza to, że rozporządzenie wchodzi w życie i jest stosowane bez względu na istniejące środki prawodawstwa krajowego: bezpośrednio do przepisów rozporządzenia mogą z reguły odwoływać się obywatele, przedsiębiorstwa, administracje publiczne i inne organizacje zajmujące się przetwarzaniem danych osobowych. Państwa członkowskie muszą jednak – zgodnie z rozporządzeniem – podjąć działania niezbędne do dostosowania swojego ustawodawstwa, a mianowicie: uchylić i zmienić obowiązujące przepisy, utworzyć krajowe organy ochrony danych[28], wybrać jednostkę akredytującą[29] oraz ustanowić przepisy mające na celu pogodzenie wolności wypowiedzi z ochroną danych[30].

Dzięki rozporządzeniu państwa członkowskie uzyskały również możliwość dalszego doprecyzowania stosowania przepisów o ochronie danych w określonych dziedzinach: sektora publicznego[31], prawa pracy i zabezpieczenia społecznego[32], profilaktyki zdrowotnej lub medycyny pracy, zdrowia publicznego[33], przetwarzania do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych[34], krajowego numeru identyfikacyjnego[35], publicznego dostępu do dokumentów urzędowych[36],

---

[27] Art. 288 TFUE.

[28] Art. 54 ust. 1 rozporządzenia.

[29] Zgodnie z art. 43 ust. 1 rozporządzenia państwa członkowskie umożliwiają podmiotom certyfikującym skorzystanie z dwóch sposobów akredytacji, tj. przez krajowy organ nadzorujący ochronę danych utworzony na mocy przepisów w dziedzinie ochrony danych lub przez krajową jednostkę akredytującą utworzoną na mocy rozporządzenia (WE) nr 765/2008 dotyczącego akredytacji i nadzoru rynku. W tym celu Europejska Współpraca w Dziedzinie Akredytacji („EA", uznana na mocy rozporządzenia nr 765/2008), w której skład wchodzą krajowe jednostki akredytujące, oraz organy nadzorcze określone w RODO powinny ściśle ze sobą współpracować.

[30] Art. 85 ust. 1 rozporządzenia.

[31] Art. 6 ust. 2 rozporządzenia.

[32] Art. 88 oraz 9 ust. 2 lit. b) rozporządzenia. Europejski filar praw socjalnych stanowi również, że „pracownicy mają prawo do ochrony swoich danych osobowych w kontekście zatrudnienia" (2017/C 428/09, Dz.U. C 428 z 13.12.2017, s. 10–15).

[33] Art. 9 ust. 2 lit. h) oraz i) rozporządzenia.

[34] Art. 9 ust. 2 lit. j) rozporządzenia.

[35] Art. 87 rozporządzenia.

[36] Art. 86 rozporządzenia.

i obowiązku zachowania tajemnicy[37]. Ponadto rozporządzenie uprawnia państwa członkowskie do zachowania lub wprowadzania dalszych warunków, w tym ograniczeń, przetwarzania danych genetycznych, danych biometrycznych lub danych dotyczących zdrowia[38].

Działania państw członkowskich w tym kontekście są ograniczone przez dwa elementy:

1. art. 8 Karty, co oznacza, że wszelkie krajowe przepisy doprecyzowujące muszą spełniać wymogi określone w art. 8 Karty (oraz rozporządzenia, które opiera się na art. 8 Karty); oraz
2. art. 16 ust. 2 TFUE, zgodnie z którym przepisy krajowe nie mogą naruszać swobodnego przepływu danych osobowych w UE.

Rozporządzenie daje możliwość uproszczenia otoczenia prawnego, czyli zmniejszenia liczby przepisów krajowych i zapewnienia podmiotom większej przejrzystości.

Dostosowując swoje przepisy krajowe, państwa członkowskie muszą wziąć pod uwagę fakt, że wszelkie działania na szczeblu krajowym, które mogłyby stworzyć przeszkody dla bezpośredniego stosowania rozporządzenia i które mogłyby zagrozić jego jednoczesnemu i jednolitemu stosowaniu w całej UE, są sprzeczne z Traktatami[39].

Zakazane jest ponadto powtarzanie treści rozporządzeń w prawie krajowym (np. powtarzanie definicji lub praw osób fizycznych), chyba że takie powtórzenia są absolutnie niezbędne, aby spójność była zachowana oraz aby przepisy krajowe były zrozumiałe dla osób, do których mają zastosowanie[40]. Dosłowne powielenie treści rozporządzenia w prawie krajowym powinno stanowić wyjątek i być uzasadnione, przy czym nie można go stosować w celu wprowadzenia dodatkowych warunków lub interpretacji do treści rozporządzenia.

Wykładnię rozporządzenia pozostawia się sądom europejskim (sądom krajowym i ostatecznie Trybunałowi Sprawiedliwości), nie prawodawcom państw członkowskich. Ustawodawca krajowy nie może zatem kopiować treści rozporządzenia, jeżeli nie jest to konieczne w świetle kryteriów określonych w orzecznictwie, ani interpretować czy wprowadzać dodatkowych warunków do przepisów mających bezpośrednie zastosowanie na mocy rozporządzenia. W takim przypadku podmioty gospodarcze w Unii byłyby bowiem znów narażone na rozdrobnienie i nie wiedziałyby, do których przepisów mają się stosować.

Na tym etapie jedynie dwa państwa członkowskie przyjęły odpowiednie ustawodawstwo krajowe[41]; w pozostałych państwach członkowskich procedura ustawodawcza znajduje się na różnych etapach zaawansowania[42], państwa te przewidziały przyjęcie odpowiedniego

[37] Art. 90 rozporządzenia.
[38] Art. 9 ust. 4 rozporządzenia.
[39] Wyrok Trybunału z dnia 31 stycznia 1978 r., Fratelli Zerbone Snc przeciwko Amministrazione delle finanze dello Stato, C-94/77, ECLI:EU:C:1978:17 oraz 101.
[40] Motyw 8 rozporządzenia.
[41] Austria (http://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2017_I_120/BGBLA_2017_I_120.pdf); Niemcy (https://www.bgbl.de/xaver/bgbl/start.xav?start=%2F%2F*%5B%40attr_id%3D%27bgbl117s2097.pdf%27%5D#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl117s2097.pdf%27%5D__1513091793362).
[42] Przegląd aktualnego stanu prac nad procesem legislacyjnym w poszczególnych państwach członkowskich jest dostępny pod adresem:

ustawodawstwa do dnia 25 maja 2018 r. Istotne jest, aby podmioty gospodarcze miały wystarczająco dużo czasu na przygotowanie się do wprowadzenia wszystkich przepisów, których będą musiały przestrzegać.

Jeżeli państwa członkowskie nie podejmą działań wymaganych na podstawie rozporządzenia, opóźnią się w ich podjęciu lub wykorzystają określone w rozporządzeniu klauzule precyzujące w sposób sprzeczny z rozporządzeniem, Komisja skorzysta ze wszystkich dostępnych narzędzi, w tym z możliwości wszczęcia postępowania w sprawie naruszenia.

3.2. Zapewnienie pełnej operacyjności nowej niezależnej Europejskiej Rady Ochrony Danych przez organy ochrony danych

Zasadnicze znaczenie ma, aby nowy organ utworzony na mocy rozporządzenia, tj. Europejska Rada Ochrony Danych[43], następca Grupy Roboczej Art. 29, osiągnął pełną zdolność operacyjną do dnia 25 maja 2018 r.

Mając na celu wzmocnienie synergii i skuteczności, Europejski Inspektor Ochrony Danych, tj. organ ochrony danych odpowiedzialny za nadzór instytucji i organów UE, zadba o sekretariat Europejskiej Rady Ochrony Danych. W tym celu w minionych miesiącach Europejski Inspektor Ochrony Danych rozpoczął niezbędne przygotowania.

Europejska Rada Ochrony Danych znajdzie się w centrum ochrony danych w Europie. Będzie ona przyczyniać się do jednolitego stosowania prawa w dziedzinie ochrony danych oraz zapewni silną podstawę współpracy między organami ochrony danych, w tym Europejskiego Inspektora Ochrony Danych. Europejska Rada Ochrony Danych będzie nie tylko wydawać wytyczne w sprawie interpretacji kluczowych pojęć rozporządzenia, ale będzie również wydawać wiążące decyzje w sporach dotyczących transgranicznego przetwarzania. Zapewni to jednolite stosowanie przepisów unijnych i zapobiegnie rozstrzyganiu tej samej sprawy w rozbieżny sposób w różnych państwach członkowskich.

Sprawne i efektywne funkcjonowanie Europejskiej Rady Ochrony Danych jest zatem warunkiem dobrego funkcjonowania systemu jako całości. Dla zapewnienia jednolitej interpretacji przepisów rozporządzenia Europejska Rada Ochrony Danych będzie musiała stworzyć wspólną kulturę ochrony danych wśród wszystkich krajowych organów ochrony danych, co będzie zadaniem intensywniejszym niż kiedykolwiek wcześniej. Rozporządzenie sprzyja współpracy między organami ochrony danych, nadając im narzędzia do skutecznej i efektywnej współpracy: w szczególności będą one w stanie przeprowadzać wspólne operacje, przyjmować decyzje w ramach porozumienia oraz rozstrzygać potencjalne rozbieżności dotyczące interpretacji rozporządzenia na forum Rady w drodze opinii i wiążących decyzji. Komisja zachęca organy ochrony danych do przyjęcia tych zmian i dostosowania swojej kultury funkcjonowania, finansowania i pracy, aby móc przyjąć nowe prawa i spełniać nowe obowiązki.

3.3. Zapewnienie przez państwa członkowskie niezbędnych zasobów finansowych i ludzkich na potrzeby organów ochrony danych

---

http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3461&Lang=PL

[43] Europejska Rada Ochrony Danych będzie organem UE posiadającym osobowość prawną i odpowiedzialnym za jednolite stosowanie rozporządzenia. W skład tego organu wchodzić będą przewodniczący wszystkich organów ochrony danych oraz Europejski Inspektor Ochrony Danych lub ich przedstawiciele.

Utworzenie w pełni niezależnych organów nadzorczych w każdym państwie członkowskim ma kluczowe znaczenie dla zapewnienia ochrony osób fizycznych w związku z przetwarzaniem ich danych osobowych w UE[44]. Organy nadzorcze nie mogą skutecznie chronić praw i wolności osób fizycznych, jeżeli nie są całkowicie niezależne. Jakiekolwiek uchybienie przy gwarantowaniu im niezależności i nadawaniu uprawnień ma daleko idący, negatywny wpływ na wykonywanie przepisów z zakresu ochrony danych[45].

W rozporządzeniu skodyfikowano wymóg, zgodnie z którym wszystkie organy ochrony danych mają działać w sposób całkowicie niezależny[46]. Zwiększa on niezależność krajowych organów ochrony danych i nadaje im jednolite uprawnienia w całej UE, tak aby posiadały one odpowiednie kompetencje do skutecznego rozpatrywania skarg, uprawnienia do przeprowadzania skutecznych dochodzeń, podejmowania wiążących decyzji i nakładania skutecznych i odstraszających sankcji. Nadano im ponadto uprawnienia do nakładania administracyjnych kar pieniężnych na administratorów czy podmioty przetwarzające w wysokości do 20 mln EUR, a w przypadku przedsiębiorstwa – w wysokości do 4 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa.

Organy ochrony danych są naturalnymi partnerami i pierwszym punktem kontaktowym dla ogółu społeczeństwa, przedsiębiorstw i administracji publicznych w przypadku pytań dotyczących rozporządzenia. Rola organów ochrony danych obejmuje informowanie administratorów i podmiotów przetwarzających o ich zobowiązaniach, a także upowszechnianie w społeczeństwie wiedzy o ryzyku, przepisach, zabezpieczeniach i prawach związanych z przetwarzaniem oraz zrozumienia tych zjawisk. Nie oznacza to jednak, że administratorzy i podmioty przetwarzające powinni oczekiwać, że organy ochrony danych zapewnią im dostosowaną do potrzeb, zindywidualizowaną opinię prawną, którą zapewnić może jedynie prawnik bądź inspektor ochrony danych.

Krajowe organy ochrony danych odgrywają kluczową rolę, jednak stosunkowy brak równowagi między zasobami ludzkimi i finansowymi, które przydziela się im w różnych państwach członkowskich, może stanowić zagrożenie dla ich skuteczności, a ostatecznie – dla ich pełnej niezależności wymaganej na podstawie rozporządzenia. Może to również mieć negatywny wpływ na sposób, w jaki organy ochrony danych mogą wykonywać swoje uprawnienia, takie jak uprawnienia w zakresie prowadzenia dochodzeń. Zachęca się państwa członkowskie do wypełnienia ich prawnego obowiązku, jakim jest zapewnienie krajowym organom ochrony danych zasobów kadrowych, technicznych i finansowych, pomieszczeń i infrastruktury niezbędnych do skutecznego wypełniania ich zadań i wykonywania ich uprawnień[47].

3.4. Przygotowywanie się przedsiębiorstw, administracji publicznych i innych organizacji przetwarzających dane do stosowania nowych przepisów

Rozporządzenie nie zmieniło w znaczący sposób głównych pojęć i zasad dotyczących przepisów w dziedzinie ochrony danych wprowadzonych w 1995 r. Oznacza to, że znaczna większość administratorów i podmiotów przetwarzających nie będzie musiała wprowadzać

[44] Motyw 117 i wcześniejsze stwierdzenie już w motywie 62 dyrektywy 95/46.
[45] Komunikat Komisji dla Parlamentu Europejskiego i Rady w sprawie kontynuacji programu prac na rzecz skuteczniejszego wdrażania dyrektywy o ochronie danych, COM(2007) 87 final z dnia 7 marca 2007 r.
[46] Art. 52 rozporządzenia.
[47] Art. 52 ust. 4 rozporządzenia.

istotnych zmian w operacjach przetwarzania danych w celu osiągnięcia zgodności z rozporządzeniem, pod warunkiem, że już teraz działają oni zgodnie z obowiązującymi w UE przepisami w zakresie ochrony danych.

Rozporządzenie ma wpływ przede wszystkim na podmioty gospodarcze, których główną działalnością gospodarczą jest przetwarzanie danych lub obchodzenie się z danymi wrażliwymi. Ma również wpływ na podmioty, które regularnie i systematycznie monitorują osoby fizyczne na dużą skalę. Te podmioty gospodarcze będą najprawdopodobniej musiały wyznaczyć inspektora ochrony danych, przeprowadzić ocenę skutków dla ochrony danych i zgłosić naruszenia ochrony danych, jeżeli istnieje zagrożenie dla praw i wolności osób fizycznych. Dla porównania, podmioty gospodarcze – w szczególności MŚP – których główna działalność nie obejmuje przetwarzania, z którym łączy się wysokie ryzyko, co do zasady nie podlegają wspomnianym szczególnym zobowiązaniom określonym w rozporządzeniu.

Istotne jest, aby administratorzy i podmioty przetwarzające podejmowali się dogłębnych przeglądów cyklu swojej polityki w zakresie danych, aby mogli wyraźnie zidentyfikować, jakie dane posiadają, do jakich celów i na jakiej podstawie prawnej (np. chmura; podmioty gospodarcze w sektorze finansowym). Muszą oni również dokonać oceny obowiązujących umów, w szczególności tych zawartych między administratorami i podmiotami przetwarzającymi, ścieżek międzynarodowego przekazywania danych i ogólnego zarządzania (stosowanych środków informatycznych i organizacyjnych), w tym wyznaczenia inspektora ochrony danych. Zasadniczym elementem w tym procesie jest zapewnienie, aby w takich przeglądach brał udział najwyższy szczebel zarządzania, wnosił swój wkład oraz aby regularnie przekazywano mu najnowsze informacje i konsultowano się z nim w sprawie zmian dotyczących polityki danych przedsiębiorstwa.

W tym celu niektóre podmioty gospodarcze korzystają z list kontrolnych odnoszących się do zgodności (wewnętrznych albo zewnętrznych), konsultują się z przedsiębiorstwami doradczymi i kancelariami prawnymi oraz poszukują produktów, które spełnią wymogi w zakresie uwzględniania ochrony danych w fazie projektowania oraz z zasadą domyślnej ochrony danych. Każdy sektor musi wypracować ustalenia odpowiednie do szczególnego charakteru swojej dziedziny i dostosowane do danego modelu biznesowego.

Przedsiębiorstwa i inne organizacje przetwarzające dane będą mogły wykorzystać nowe narzędzia przewidziane w rozporządzeniu również jako element wykazania zgodności, np. kodeksy postępowania i mechanizmy certyfikacji. Chodzi to o podejścia oddolne, które wywodzą się ze środowiska biznesu, stowarzyszeń i innych organizacji reprezentujących kategorie administratorów i podmiotów przetwarzających oraz odzwierciedlają najlepsze praktyki, istotne zmiany w danym sektorze, lub które mogą informować o poziomie ochrony danych wymaganym przez niektóre produkty i usługi. W rozporządzeniu przewidziano uproszczony zbiór przepisów dotyczących takich mechanizmów, biorąc pod uwagę realia rynkowe (np. certyfikacje udzielone przez podmiot certyfikujący lub przez organ ochrony danych).

Wprawdzie duże przedsiębiorstwa czynnie przygotowują się do stosowania nowych przepisów, jednak wiele MŚP nie jest w pełni świadomych nadchodzących przepisów o ochronie danych.

Krótko mówiąc, podmioty gospodarcze powinny przygotować i dostosować się do nowych przepisów oraz postrzegać rozporządzenie jako:

- możliwość przywrócenia prawidłowości w funkcjonowaniu przedsiębiorstwa, jeżeli chodzi o rodzaj przetwarzanych danych osobowych i sposób zarządzania nimi;
- zobowiązanie do opracowania produktów sprzyjających prywatności i ochronie danych oraz budowania z klientami nowych relacji opierających się na przejrzystości i zaufaniu; oraz
- możliwość podjęcia na nowo stosunków z organami ochrony danych poprzez rozliczalność i aktywne przestrzeganie przepisów.

3.5. Informowanie zainteresowanych stron, w szczególności obywateli oraz małych i średnich przedsiębiorstw

Powodzenie rozporządzenia zależy od właściwej świadomości wszystkich podmiotów, których dotyczą nowe przepisy (środowiska biznesu i innych organizacji przetwarzających dane, sektora publicznego i obywateli). Jeżeli chodzi o szczebel krajowy, zadanie podnoszenia świadomości i obowiązek stanowienia pierwszego punktu kontaktowego dla administratorów, podmiotów przetwarzających i osób fizycznych należy przede wszystkim do organów ochrony danych. Jako organy egzekwowania przepisów o ochronie danych na swoim terytorium, organy ochrony danych są również najwłaściwsze do wyjaśniania przedsiębiorstwom i sektorowi publicznemu zmian wprowadzonych rozporządzeniem oraz do zapoznania obywateli z ich prawami.

Organy ochrony danych rozpoczęły informowanie zainteresowanych stron zgodnie z odpowiednim podejściem krajowym. Niektóre państwa organizują seminaria z udziałem administracji publicznych, zarówno na szczeblu regionalnym, jak i lokalnym, oraz prowadzą warsztaty dla różnych sektorów gospodarczych w celu podniesienia świadomości w zakresie głównych przepisów rozporządzenia. Niektóre prowadzą tematyczne programy szkoleniowe dla inspektorów ochrony danych. Większość z nich udostępnia na swoich stronach internetowych materiały informacyjne w różnych formatach (listy kontrolne, wideo itp.).

Świadomość zmian i większych praw, które wprowadzą przepisy o ochronie danych, wciąż nie jest jednak wystarczająco rozpowszechniona wśród obywateli. Należy kontynuować i zintensyfikować uruchomioną przez organy ochrony danych inicjatywę na rzecz szkoleń i podnoszenia świadomości, skupiając się przede wszystkim na MŚP. Ponadto krajowe administracje sektorowe mogą wspierać działania organów ochrony danych i – w oparciu o uzyskane od nich informacje – prowadzić własne działania informacyjne skierowane do różnych zainteresowanych stron.

4. KOLEJNE KROKI

W ciągu najbliższych miesięcy Komisja będzie aktywnie wspierać wszystkie podmioty w przygotowaniu do stosowania rozporządzenia.

a) Współpraca z państwami członkowskimi

Komisja będzie kontynuować współpracę z państwami członkowskimi w ramach przygotowania do zmian, które wejdą w życie w maju 2018 r. Począwszy od maja 2018 r. Komisja będzie monitorować sposób stosowania nowych przepisów przez państwa członkowskie i – w razie potrzeby – podejmować odpowiednie działania.

b) Nowe wytyczne dostępne w internecie we wszystkich językach UE i działania związane z podnoszeniem świadomości

Komisja udostępnia praktyczne wytyczne[48], aby pomóc przedsiębiorcom, w szczególności MŚP, a także organom publicznym i społeczeństwu w przestrzeganiu nowych przepisów o ochronie danych i w korzystaniu z nich.

Wytyczne mają postać praktycznego narzędzia internetowego, które jest dostępne we wszystkich językach UE. To narzędzie internetowe będzie regularnie aktualizowane i ma służyć trzem głównym grupom odbiorców docelowych: obywatelom, przedsiębiorstwom (w szczególności MŚP) i innym organizacjom oraz organom administracji publicznej. Zawiera ono pytania i odpowiedzi wybrane na podstawie informacji zwrotnych otrzymanych od zainteresowanych stron, a także praktyczne przykłady i odniesienia do różnych źródeł informacji (np. do artykułów rozporządzenia, wytycznych Grupy Roboczej Art. 29 / Europejskiej Rady Ochrony Danych, jak również do materiałów opracowanych na szczeblu krajowym).

Komisja będzie dokonywać regularnych aktualizacji tego narzędzia, uzupełniając pytania i aktualizując odpowiedzi, w oparciu o otrzymane informacje zwrotne i w świetle wszelkich nowych kwestii pojawiających się w trakcie wdrażania.

Wytyczne będą promowane za pośrednictwem kampanii informacyjnej i działań w zakresie rozpowszechniania prowadzonych we wszystkich państwach członkowskich, skierowanych do przedsiębiorstw i społeczeństwa.

Rozporządzenie przewiduje silniejsze prawa osób fizycznych, Komisja zaangażuje się również w działania z zakresu podnoszenia świadomości i będzie uczestniczyć w wydarzeniach odbywających się w poszczególnych państwach członkowskich, aby informować obywateli o korzyściach płynących z rozporządzenia oraz o jego oddziaływaniu.

c) Wsparcie finansowe dla krajowych kampanii i działań z zakresu podnoszenia świadomości

Komisja wspiera podejmowane na szczeblu krajowym wysiłki mające na celu podnoszenie świadomości i zapewnienie przestrzegania przepisów, przyznając dotacje, które mogą zostać wykorzystane do organizowania szkoleń dla pracowników organów ochrony danych i organów administracji publicznej, przedstawicieli zawodów prawniczych oraz dla inspektorów ochrony danych[49], jak również do zapoznania ich z rozporządzeniem.

Około 1,7 mln EUR zostanie przyznane sześciu beneficjentom, których obszar działania obejmuje ponad połowę państw członkowskich. Finansowanie będzie skierowane do organów publicznych, w tym do inspektorów ochrony danych podlegających pod władze lokalne i organy publiczne, oraz do inspektorów z sektora prywatnego, sędziów i prawników. Dotacje będą wykorzystywane do rozszerzania materiałów szkoleniowych przeznaczonych dla organów ochrony danych, inspektorów ochrony danych i innych specjalistów, a także dla programów szkoleń przeznaczonych dla osób prowadzących szkolenia.

---

[48] Wytyczne przyczynią się do lepszego zrozumienia unijnych przepisów o ochronie danych, ale moc prawną ma jedynie tekst rozporządzenia. A zatem wyłącznie na mocy rozporządzenia można ustanawiać prawa i obowiązki względem osób fizycznych.

[49] Dotacje przyznane w ramach programu „Prawa, równość i obywatelstwo”: https://ec.europa.eu/research/participants/portal/desktop/en/opportunities/rec/calls/rec-data-2016.html#c,topics=callIdentifier/t/REC-DATA-2016/1/1/1/default-group&callStatus/t/Forthcoming/1/1/0/default-group&callStatus/t/Open/1/1/0/default-group&callStatus/t/Closed/1/1/0/default-group&+identifier/desc

Komisja wystosowała również zaproszenie do składania wniosków skierowane specjalnie do organów ochrony danych. Całkowity budżet dotacji wyniesie do 2 mln EUR, a środki te wspomogą organy ochrony danych w dotarciu do zainteresowanych stron[50]. Mają one na celu zapewnienie współfinansowania – na poziomie 80 % – środków, które będą stosowane przez organy ochrony danych w latach 2018–2019 w celu podnoszenia świadomości wśród przedsiębiorstw, w szczególności MŚP, i odpowiadania na ich pytania. Finansowanie to można wykorzystać również do podnoszenia świadomości w społeczeństwie.

d) Ocena zapotrzebowania na wykorzystanie uprawnień Komisji

Na mocy rozporządzenia[51] Komisja otrzymuje uprawnienie do wydawania aktów wykonawczych lub delegowanych w celu dalszego wsparcia wdrażania nowych przepisów. Komisja będzie korzystać z tych uprawnień tylko wtedy, gdy ich użycie wyraźnie wytworzy wartość dodaną, i w oparciu o informacje zwrotne uzyskane w drodze konsultacji z zainteresowanymi stronami. W szczególności Komisja zbada kwestię certyfikacji, opierając się na badaniu zleconym ekspertom zewnętrznym oraz na informacjach i wskazówkach na ten temat, które uzyskano od grupy reprezentującej różne zainteresowane strony, powołanej ds. rozporządzenia pod koniec 2017 r. W tym kontekście istotne będą również działania podejmowane przez Agencję Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA) w dziedzinie cyberbezpieczeństwa.

e) Włączenie rozporządzenia do Porozumienia EOG

Komisja będzie kontynuować współpracę z państwami EFTA (Islandią, Liechtensteinem i Norwegią) w ramach Europejskiego Obszaru Gospodarczego (EOG) w celu włączenia rozporządzenia do Porozumienia EOG[52]. Dopiero kiedy rozporządzenie zostanie prawomocnie włączone do Porozumienia EOG, dane osobowe będą mogły swobodnie przepływać między państwami UE i EOG w taki sam sposób, w jaki przepływają między państwami członkowskimi UE.

f) Wyjście Zjednoczonego Królestwa z UE

W kontekście prowadzonych między UE a Zjednoczonym Królestwem negocjacji w sprawie umowy o wystąpieniu na podstawie art. 50 Traktatu o Unii Europejskiej celem Komisji będzie zapewnienie, aby przepisy prawa Unii o ochronie danych osobowych, które mają zastosowanie w dniu poprzedzającym wystąpienie, w dalszym ciągu miały zastosowanie dla danych osobowych przetworzonych w Zjednoczonym Królestwie przed datą wystąpienia[53].

---

[50] http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/rec/topics/rec-rdat-trai-ag-2017.html

[51] Akt delegowany w sprawie przedstawiania informacji za pomocą znaków graficznych i procedur opracowywania standardowych znaków graficznych (art. 12 ust. 8 rozporządzenia); akt delegowany w sprawie wymogów, które należy uwzględnić w mechanizmie certyfikacji (art. 43 ust. 8 rozporządzenia); akt wykonawczy w sprawie określania technicznych standardów mechanizmów certyfikacji oraz znaków jakości i oznaczeń w dziedzinie ochrony danych, a także sposobów upowszechniania i uznawania tych mechanizmów certyfikacji oraz znaków jakości i oznaczeń (art. 43 ust. 9 rozporządzenia); akt wykonawczy w sprawie formatu i procedur wymiany informacji między administratorami, podmiotami przetwarzającymi i organami nadzorczymi do celów wiążących reguł korporacyjnych (art. 47 ust. 3 rozporządzenia); akty wykonawcze w sprawie formatu i procedur wzajemnej pomocy i wymiany informacji drogą elektroniczną między organami nadzorczymi (art. 61 ust. 9 i art. 67 rozporządzenia).

[52] Aby uzyskać dodatkowe informacje na temat aktualnej sytuacji, zob.: http://www.efta.int/eea-lex/32016R0679

[53] https://ec.europa.eu/commission/publications/position-paper-use-data-and-protection-information-obtained-or-processed-withdrawal-date_en

Na przykład osoby fizyczne, których ta sytuacja dotyczy, powinny dalej posiadać prawo do informacji, prawo dostępu, prawo do sprostowania, usunięcia, do ograniczenia przetwarzania, do przenoszenia danych, prawo do sprzeciwu wobec przetwarzania, a także do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu – na podstawie odpowiednich przepisów prawa Unii, które mają zastosowanie w dniu wystąpienia. Wskazane powyżej dane osobowe nie mogą być przechowywane dłużej niż jest to konieczne dla celów, dla których te dane osobowe zostały przetworzone.

Z dniem wystąpienia – oraz przy uwzględnieniu wszelkich przepisów przejściowych, które mogą zostać zawarte w możliwej umowie o wystąpieniu – wobec Zjednoczonego Królestwa będą miały zastosowanie przepisy rozporządzenia dotyczące przekazów danych osobowych do państw trzecich[54].

g) Podsumowanie postępów w maju 2019 r.

Po dniu 25 maja 2018 r. Komisja będzie ściśle monitorować stosowanie nowych przepisów i będzie gotowa do podjęcia działań, jeżeli pojawią się jakiekolwiek znaczące problemy. Po upływie roku od wejścia w życie rozporządzenia (w 2019 r.) Komisja zorganizuje wydarzenie, podczas którego będzie możliwe podsumowanie doświadczeń różnych zainteresowanych stron w zakresie wdrażania rozporządzenia. Te informacje będą również przydatne w sporządzeniu sprawozdania, które Komisja musi opracować do maja 2020 r. i które ma dotyczyć oceny i przeglądu rozporządzenia. Sprawozdanie to skupi się w szczególności na międzynarodowym przekazywaniu danych i na przepisach dotyczących współpracy i spójności, które mają związek z działalnością organów ochrony danych.

Podsumowanie

W dniu 25 maja w całej UE wejdzie w życie nowy jednolity zestaw przepisów o ochronie danych. Nowe ramy przyniosą znaczne korzyści zarówno osobom fizycznym, przedsiębiorstwom, organom administracji publicznej, jak i innym organizacjom. Stwarza to UE także okazję przekształcenia się w światowego lidera ochrony danych osobowych. Niemniej reforma może odnieść sukces tylko wtedy, gdy wszystkie zaangażowane strony zaakceptują swoje obowiązki i swoje prawa.

Od czasu przyjęcia rozporządzenia w maju 2016 r. Komisja prowadziła aktywny dialog ze wszystkimi zainteresowanymi podmiotami: rządami, organami krajowymi, przedsiębiorstwami, organizacjami społeczeństwa obywatelskiego, dotyczący stosowania nowych przepisów. Włożono wprawdzie bardzo dużo pracy w zapewnienie wysokiego poziomu świadomości i pełnej gotowości, jest jednak jeszcze wiele do zrobienia. Państwa członkowskie i różne zainteresowane strony przygotowują się w różnym tempie. Ponadto wiedza na temat korzyści i możliwości, które przynoszą nowe przepisy, nie wszędzie jest tak samo rozpowszechniona. Szczególnie konieczne jest podniesienie świadomości i wsparcie działań na rzecz przestrzegania przepisów przez MŚP.

W związku z tym Komisja wzywa wszystkie zainteresowane strony do zintensyfikowania prowadzonych działań, aby zapewnić spójne stosowanie i interpretację nowych przepisów w całej UE i podnieść świadomość zarówno wśród przedsiębiorstw, jak i obywateli. Komisja

[54] Zobacz zawiadomienie Komisji dla zainteresowanych stron: przepisy dotyczące wyjścia Zjednoczonego Królestwa z UE w dziedzinie ochrony danych (http://ec.europa.eu/newsroom/just/document.cfm?action=display&doc_id=49245).

będzie wspierać te wysiłki, zapewniając finansowanie i wsparcie administracyjne. Komisja pomoże także w podnoszeniu ogólnej świadomości, szczególnie poprzez uruchomienie zestawu narzędzi internetowych.

Dane stają się bardzo cenne dla współczesnej gospodarki i są bardzo istotne w codziennym życiu obywateli. Nowe przepisy stanowią wyjątkową szansę zarówno dla przedsiębiorstw, jak i dla społeczeństwa. Przedsiębiorstwa – szczególnie mniejsze – będą mogły skorzystać z jednolitego, sprzyjającego innowacji zestawu przepisów i uporządkować swoje rozwiązania w kwestii danych osobowych, aby odzyskać zaufanie konsumentów i wykorzystać je jako przewagę konkurencyjną w UE. Obywatele skorzystają z silniejszej ochrony danych osobowych i uzyskają większą kontrolę nad sposobem, w jaki przedsiębiorstwa obchodzą się z danymi.

We współczesnym świecie, w którym dokonuje się gwałtowny rozwój gospodarki cyfrowej, Unia Europejska, jej obywatele i przedsiębiorstwa muszą dysponować wyposażeniem umożliwiającym czerpanie korzyści z gospodarki opartej na danych i zrozumienie jej wpływu. Rozporządzenie zapewnia narzędzia niezbędne do przygotowania Europy na XXI wiek.

Komisja podejmie następujące działania:

Wobec państw członkowskich

- Komisja będzie dalej współpracować z państwami członkowskimi w celu wspierania spójności i ograniczenia fragmentacji w stosowaniu rozporządzenia, uwzględniając swobodę w doprecyzowaniu przepisów, którą daje państwom członkowskim nowe prawodawstwo;

- począwszy od maja 2018 r. Komisja będzie ściśle monitorować stosowanie rozporządzenia w państwach członkowskich i w razie potrzeby podejmować odpowiednie działania, w tym działania w odpowiedzi na naruszenia przepisów;

Wobec organów ochrony danych

- do maja 2018 r. Komisja będzie wspierać działania organów ochrony danych w kontekście Grupy Roboczej Art. 29 i okresu przejściowego przed rozpoczęciem funkcjonowania Europejskiej Rady Ochrony Danych; od maja 2018 r. będzie pomagać Europejskiej Radzie Ochrony Danych w jej pracy;

- w latach 2018–2019 Komisja będzie współfinansować (całkowity budżet wyniesie do 2 mln EUR) działania związane z podnoszeniem świadomości prowadzone przez organy ochrony danych na szczeblu krajowym (projekty realizowane od połowy 2018 r.);

Wobec zainteresowanych stron

- Komisja przygotuje praktyczne narzędzie internetowe dostarczające porad, w którym zawarte będą pytania i odpowiedzi ukierunkowane na obywateli, przedsiębiorstwa i organy administracji publicznej. Komisja zamierza promować te wytyczne wśród odbiorców docelowych, prowadząc kampanię informacyjną skierowaną do przedsiębiorstw i społeczeństwa zarówno w okresie poprzedzającym maj 2018 r., jaki

i później;

- w 2018 r. i w latach kolejnych Komisja będzie nadal prowadzić aktywny dialog z zainteresowanymi stronami, szczególnie za pośrednictwem grupy reprezentującej różne zainteresowane strony, dotyczący wdrożenia rozporządzenia i poziomu świadomości w zakresie nowych przepisów;

Wobec wszystkich podmiotów

- w latach 2018–2019 Komisja oceni, czy będzie musiała wykorzystać swoje uprawnienia do przyjmowania aktów delegowanych lub wykonawczych;

- w maju 2019 r. Komisja dokona podsumowania wdrażania rozporządzenia, a w 2020 r. przygotuje sprawozdanie w sprawie stosowania nowych przepisów.

KOMISJA
EUROPEJSKA

Bruksela, dnia 24.6.2020 r.
COM(2020) 264 final

KOMUNIKAT KOMISJI DO PARLAMENTU EUROPEJSKIEGO I RADY

Ochrona danych jako filar wzmacniania pozycji obywateli oraz podejścia UE do transformacji cyfrowej – dwa lata stosowania ogólnego rozporządzenia o ochronie danych

{SWD(2020) 115 final}

KOMUNIKAT KOMISJI DO PARLAMENTU EUROPEJSKIEGO I RADY

Ochrona danych jako filar wzmacniania pozycji obywateli oraz podejście UE do transformacji cyfrowej – dwa lata stosowania ogólnego rozporządzenia o ochronie danych

1 PRZEPISY O OCHRONIE DANYCH JAKO FILAR WZMACNIANIA POZYCJI OBYWATELI ORAZ PODEJŚCIE UE DO TRANSFORMACJI CYFROWEJ

Niniejsze sprawozdanie jest pierwszym sprawozdaniem z oceny i przeglądu ogólnego rozporządzenia o ochronie danych[1] (zwanego dalej „RODO"), w szczególności w odniesieniu do stosowania i funkcjonowania przepisów dotyczących przekazywania danych osobowych do państw trzecich i organizacji międzynarodowych oraz przepisów dotyczących współpracy i spójności zgodnie z art. 97 RODO.

Ogólne rozporządzenie o ochronie danych (RODO), które obowiązuje od dnia 25 maja 2018 r., stanowi centralny element unijnych ram[2] gwarantujących podstawowe prawo do ochrony danych, zapisane w Karcie praw podstawowych Unii Europejskiej (art. 8) i w traktatach (art. 16 Traktatu o funkcjonowaniu Unii Europejskiej, „TFUE"). Dzięki wprowadzeniu RODO wzmocniono gwarancje ochrony danych, zapewniono obywatelom dodatkowe i większe prawa oraz większą przejrzystość, a także zagwarantowano, że wszystkie podmioty wykorzystujące dane osobowe objęte zakresem stosowania tego rozporządzenia podlegają większej odpowiedzialności. W rozporządzeniu tym wyposażono niezależne organy ochrony danych w większe i zharmonizowane uprawnienia w zakresie egzekwowania prawa oraz ustanowiono nowy system zarządzania. Ustanowiono w nim także równe warunki działania dla wszystkich przedsiębiorstw działających na rynku UE, niezależnie od miejsca ich siedziby, oraz zapewniono swobodny przepływ danych w UE, wzmacniając tym samym rynek wewnętrzny.

RODO jest ważnym elementem ukierunkowanego na człowieka podejścia do technologii i jednocześnie nadaje kierunek w wykorzystywaniu technologii w transformacji ekologicznej i cyfrowej, które charakteryzują kształtowanie polityki UE. Zostało to ostatnio podkreślone w białej księdze w sprawie sztucznej inteligencji[3]

---

[1] Rozporządzenie (UE) 2016/679 Parlamentu Europejskiego i Rady 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.U. L 119 z 4.5.2016, s. 1.

[2] Po włączeniu go do Porozumienia o Europejskim Obszarze Gospodarczym (EOG) rozporządzenie stosuje się również do Norwegii, Islandii i Liechtensteinu.

[3] https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en

i w komunikacie w sprawie europejskiej strategii w zakresie danych[4] (zwanej dalej „strategią w zakresie danych") z lutego 2020 r.

W gospodarce, która w coraz większym stopniu opiera się na przetwarzaniu danych, w tym danych osobowych, RODO stanowi istotne narzędziem gwarantujące, że osoby fizyczne mają większą kontrolę nad swoimi danymi osobowymi i że dane te są przetwarzane do celów zgodnych z prawem, w sposób legalny, uczciwy i przejrzysty. Jednocześnie RODO przyczynia się do wspierania godnych zaufania innowacji, zwłaszcza dzięki podejściu opartym na analizie ryzyka i zasadom takim jak uwzględnianie ochrony prywatności już w fazie projektowania oraz domyślna ochrona prywatności. Komisja zaproponowała uzupełnienie ram prawnych dotyczących ochrony danych i prywatności[5] za pomocą rozporządzenia o prywatności i łączności elektronicznej[6], które ma zastąpić obecną dyrektywę o prywatności i łączności elektronicznej[7]. Wniosek ten jest obecnie analizowany przez współprawodawców i jego szybkie przyjęcie jest bardzo istotne.

W ramach priorytetów Komisji w zakresie „Europy na miarę ery cyfrowej"[8] i „Europejskiego Zielonego Ładu"[9] można opracować nowe inicjatywy umożliwiające obywatelom odgrywanie bardziej aktywnej roli w transformacji cyfrowej oraz w wykorzystywaniu narzędzi cyfrowych w dążeniu do społeczeństwa neutralnego dla klimatu i do bardziej zrównoważonego rozwoju. W RODO ustanowiono ramy dla tych inicjatyw i zagwarantowano, że mają one na celu skuteczne wzmocnienie pozycji osób fizycznych.

W ramach strategii w zakresie danych[10] wezwano do utworzenia „wspólnej europejskiej przestrzeni danych", prawdziwie jednolitego rynku danych, a także dziesięciu wspólnych europejskich sektorowych przestrzeni danych istotnych w kontekście transformacji ekologicznej i cyfrowej[11]. Dla wszystkich tych priorytetów kluczowe znaczenie mają jasne i wykonalne ramy wymiany danych i zwiększenia dostępności danych. W ramach strategii w zakresie danych ogłoszono również zamiar zbadania przez Komisję w przyszłym prawodawstwie, w jaki sposób należałoby

---

[4] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_pl

[5] Te ramy prawne obejmują również dyrektywę o ochronie danych w sprawach karnych (dyrektywę 2016/680) oraz rozporządzenie o ochronie danych w odniesieniu do instytucji i organów UE (rozporządzenie 2018/1725).

[6] Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej i uchylającego dyrektywę 2002/58/WE (rozporządzenie w sprawie prywatności i łączności elektronicznej), COM(2017) 10 final – 2017/03(COD).

[7] 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.

[8] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_pl

[9] Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiej, Rady, Komitetu Ekonomiczno-Społecznego i Komitetu Regionów – Europejski Zielony Ład (COM(2019) 640 final).

[10] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „Europejska strategia w zakresie danych", COM(2020) 66 final.

[11] Przestrzenie sektorowe obejmują takie obszary jak: zdrowie, produkcja przemysłowa, energia, mobilność, rolnictwo, dane finansowe, administracja publiczna, wspólny europejski obszar danych dotyczących umiejętności, wspólna europejska przestrzeń danych dotyczących Zielonego Ładu oraz europejska chmura dla otwartej nauki.

umożliwić wykorzystanie danych przechowywanych w publicznych bazach danych do celów badań naukowych w sposób zgodny z RODO. Przestrzenie danych mają być wspierane przez europejską federację chmury obliczeniowej, co zapewni przetwarzanie danych i usługi w zakresie infrastruktury chmury obliczeniowej w zgodzie z RODO. RODO zapewnia wysoki poziom ochrony danych osobowych i centralną rolę osób fizycznych we wszystkich tych przestrzeniach danych, zapewniając jednocześnie niezbędną elastyczność umożliwiającą uwzględnienie różnych podejść.

Potrzeba zapewnienia zaufania i zapotrzebowania na ochronę danych osobowych z pewnością nie jest ograniczona do UE. Osoby fizyczne na całym świecie w coraz większym stopniu doceniają prywatność i bezpieczeństwo swoich danych. Jak wykazano w ramach niedawno przeprowadzanego badania globalnego[12], uważają one, że jest to istotny czynnik wpływający na ich decyzje dotyczące zakupu i zachowania w internecie. Rosnąca liczba przedsiębiorstw odpowiada na to zapotrzebowanie na prywatność, na przykład przez dobrowolne rozszerzanie zakresu niektórych praw i zabezpieczeń przewidzianych w RODO na ich klientów spoza UE. Wiele przedsiębiorstw propaguje również poszanowanie danych osobowych jako element przewagi konkurencyjnej i mocny atut na światowym rynku, oferując innowacyjne produkty i usługi za pomocą nowatorskich rozwiązań w zakresie prywatności lub bezpieczeństwa danych. Ponadto zwiększenie zdolności podmiotów sektora prywatnego i publicznego do gromadzenia i przetwarzania danych na dużą skalę nasuwa ważne i złożone pytania, które w coraz większym stopniu stawiają prywatność w centrum debaty publicznej w różnych częściach świata.

Przyjęcie ogólnego rozporządzenia o ochronie danych przyczyniło się do tego, że inne państwa w wielu regionach świata również podjęły działania w tej kwestii. Jest to prawdziwie globalny trend, począwszy od Chile po Koreę Południową, od Brazylii po Japonię, od Kenii po Indie oraz od Kalifornii po Indonezję. Przywództwo UE w dziedzinie ochrony danych pokazuje, że może ona działać jako globalny organ normalizacyjny w odniesieniu do regulacji gospodarki cyfrowej; fakt ten został pozytywnie przyjęty przez ważnych członków społeczności międzynarodowej, takich jak sekretarz generalny ONZ António Guterres, który stwierdził, że RODO daje „dobry przykład, […] który inspiruje do podejmowania podobnych działań w innych częściach świata", oraz zaapelował „do UE i jej państw członkowskich, by nadal prowadziły do kształtowania ery cyfrowej i odgrywały wiodącą rolę w zakresie innowacji technologicznych i regulacji.[13]

Obecny kryzys związany z COVID-19 stanowi żywy obraz tej globalizacji debaty na temat ochrony prywatności zarówno w czasie kryzysu, jak i w kontekście przyszłego świata po wyjściu z niego. Kilka państw członkowskich UE podjęło działania nadzwyczajne w celu ochrony zdrowia publicznego. RODO wyraźnie podkreśla, że

---

[12] Zob. np. badanie na temat prywatności konsumentów Cisco 2019 (https://www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-series-2019-cps.pdf). Według tego badania obejmującego ankietę przeprowadzoną wśród 2 600 konsumentów na całym świecie duże grono konsumentów podjęło już działania w celu ochrony swojej prywatności, na przykład zmieniając firmę lub dostawców ze względu na ich politykę w zakresie danych lub praktyki w zakresie wymiany danych.

[13] Przemówienie Sekretarza Generalnego ONZ w Senacie Włoch, 18 grudnia 2019 r. (dokument dostępny na stronie: https://www.un.org/press/en/2019/sgsm19916.doc.htm).

wszelkie ograniczenia muszą być zgodne z istotą podstawowych praw i wolności oraz być środkiem niezbędnym i proporcjonalnym w społeczeństwie demokratycznym, który służy do celów ochrony interesu publicznego takiego jak zdrowie publiczne. W związku z tym, że środki izolacji są stopniowo znoszone, decydenci muszą odpowiedzieć na oczekiwania obywateli co do oferty rozwiązań cyfrowych, które są godne zaufania i respektują prawa do prywatności i ochrony danych osobowych.

W wielu krajach wbudowane w system środki ochrony prywatności, takie jak dobrowolne zapisywanie się przez użytkowników, minimalizacja danych i ochrona danych, a także wyłączenie geolokalizacji, uznaje się za niezbędne do zapewnienia wiarygodności i społecznej akceptacji rozwiązań opartych na danych mających na celu monitorowanie i ograniczenie rozprzestrzeniania się wirusa, kalibrację środków przeciwdziałania w zakresie polityki publicznej, pomoc pacjentom lub wdrażanie strategii wyjścia. W UE ramy prawne dotyczące ochrony danych i prywatności[14] okazały się wystarczająco elastycznym narzędziem umożliwiającym opracowanie praktycznych rozwiązań (np. aplikacji do śledzenia kontaktów) przy jednoczesnym zapewnieniu wysokiego poziomu ochrony danych osobowych. W tym kontekście w dniu 16 kwietnia 2020 r. Komisja opublikowała wytyczne dotyczące aplikacji wspierających walkę z pandemią w odniesieniu do ochrony danych[15].

Ochrona danych osobowych ma również zasadnicze znaczenie dla zapobiegania manipulacjom w zakresie wyborów dokonywanych przez obywateli, w szczególności poprzez mikrotargetowanie wyborców w oparciu o niezgodne z prawem przetwarzanie danych osobowych, unikanie ingerencji w procesy demokratyczne oraz zachowanie otwartej debaty, sprawiedliwości i przejrzystości, które są niezbędne w demokracji. Z tego względu we wrześniu 2018 r. Komisja opublikowała wytyczne w sprawie stosowania unijnych przepisów o ochronie danych w kontekście wyborczym[16].

W ramach tej oceny i przeglądu Komisja wzięła pod uwagę wkład Rady[17], Parlamentu Europejskiego[18], Europejskiej Rady Ochrony Danych (zwanej dalej „EROD")[19] oraz indywidualnych organów ochrony danych[20], grupy ekspertów

[14] Ramy te, oprócz RODO, obejmują dyrektywę o prywatności i łączności elektronicznej (dyrektywa 2002/58/WE), która obejmuje m.in. przepisy dotyczące dostępu do informacji na temat urządzeń końcowych użytkownika i przechowywania takich informacji.

[15] Komunikat Komisji zatytułowany „Wytyczne dotyczące aplikacji pomocnych w walce z pandemią COVID-19 w odniesieniu do ochrony danych", 2020/C 124 I/01 – C/2020/2523 – Dz.U. C 124I z 17.4.2020, s. 1. W dniu 16 kwietnia 2020 r. państwa członkowskie UE, przy wsparciu Komisji, opracowały zestaw narzędzi UE na potrzeby wykorzystywania aplikacji mobilnych do śledzenia kontaktów i ostrzegania w odpowiedzi na pandemię koronawirusa. Jest to część wspólnego skoordynowanego podejścia mającego na celu wspieranie stopniowego znoszenia środków izolacji. https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf.

[16] Wytyczne Komisji dotyczące stosowania unijnych przepisów o ochronie danych osobowych w kontekście wyborczym – wkład Komisji Europejskiej na spotkanie przywódców w Salzburgu w dniach 19–20 września 2018 r. - COM(2018) 638 final.

[17] Stanowisko Rady i ustalenia w sprawie stosowania ogólnego rozporządzenia o ochronie danych: https://data.consilium.europa.eu/doc/document/ST-14994-2019-REV-2/pl/pdf.

[18] Pismo Komisji LIBE Parlamentu Europejskiego z dnia 21 lutego 2020 r. skierowane do komisarza Reyndersa, nr ref.: IPOL-COM-LIBE D (2020)6525.

[19] Wkład EROD w ocenę ogólnego rozporządzenia o ochronie danych na mocy art. 97, przyjęty w dniu 18 lutego 2020 r.: https://edpb.europa.eu/our-work-tools/our-documents/other/contribution-edpb-evaluation-gdpr-under-article-97_pl.

z udziałem wielu zainteresowanych stron[21] i innych zainteresowanych stron, w tym informacje zwrotne przekazane w odniesieniu do planu działania[22].

Ogólny pogląd jest taki, że dwa lata po wejściu w życie RODO z powodzeniem realizuje swoje cele polegające na wzmocnieniu ochrony prawa jednostki do ochrony danych osobowych i zagwarantowaniu swobodnego przepływu danych osobowych w UE [23]. Stwierdzono jednak również szereg obszarów, w których można by wprowadzić pewne ulepszenia. Podobnie jak większość zainteresowanych stron i organów ochrony danych Komisja jest zdania, że na obecnym etapie przedwczesne byłoby wyciąganie ostatecznych wniosków dotyczących stosowania RODO. Jest prawdopodobne, że przy rozwiązywaniu większości problemów wskazanych przez państwa członkowskie i zainteresowane strony będzie pomoże większe doświadczenie w stosowaniu RODO w nadchodzących latach. Niemniej jednak w niniejszym sprawozdaniu przedstawiono wyzwania napotkane do tej pory przy stosowaniu RODO oraz możliwe sposoby rozwiązania tych problemów.

Poza skupieniem się na dwóch kwestiach, o których mowa w art. 97 ust. 2 RODO, a mianowicie na przekazywaniu danych osobowych do państw trzecich lub organizacji międzynarodowych oraz na mechanizmach współpracy i spójności, w ramach tej oceny i przeglądu przyjęto również szersze podejście do kwestii poruszonych przez różne podmioty w ciągu ostatnich dwóch lat.

2 GŁÓWNE WNIOSKI

Egzekwowanie RODO oraz funkcjonowanie mechanizmu współpracy i spójności

W ramach RODO ustanowiono innowacyjny system zarządzania w oparciu o niezależne organy ochrony danych w państwach członkowskich i ich współpracę w sprawach transgranicznych oraz w ramach Europejskiej Rady Ochrony Danych („EROD"). Ogólnie uważa się, że organy ochrony danych w sposób zrównoważony wykorzystały swoje wzmocnione uprawnienia naprawcze, w tym ostrzeżenia i upomnienia, grzywny oraz ograniczenia czasowe lub definitywne dotyczące przetwarzania danych[24]. Komisja zauważa, że organy stosowały kary administracyjne wynoszące od kilku tysięcy do kilku milionów euro, w zależności od wagi naruszeń. Inne sankcje, takie jak zakaz przetwarzania danych, mogą wywołać taki sam, jeżeli nie większy, efekt odstraszający, co grzywny. Ostatecznym celem RODO jest zmiana kultury i zachowania wszystkich zaangażowanych podmiotów z korzyścią dla obywateli. Bardziej szczegółowe informacje na temat wykorzystania uprawnień naprawczych przez organy ochrony danych przedstawiono w towarzyszącym dokumencie roboczym służb Komisji.

---

[20] https://edpb.europa.eu/individual-replies-data-protection-supervisory-authorities_pl

[21] Utworzona przez Komisję wielostronna grupa ekspertów ds. rozporządzenia 2016/679 obejmuje przedstawicieli społeczeństwa obywatelskiego i przedsiębiorców, pracowników akademickich i praktyków: https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3537.

[22] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12322-Report-on-the-application-of-the-General-Data-Protection-Regulation/feedback?p_id=7669437

[23] Zob. np. stanowisko i ustalenia Rady oraz wkład EROD.

[24] Zob. pkt 2.1 dokumentu roboczego służb Komisji.

Choć wciąż jest zbyt wcześnie na pełną ocenę funkcjonowania nowych mechanizmów współpracy i spójności, organy ochrony danych zacieśniły współpracę poprzez mechanizm kompleksowej obsługi[25] i szerokie wykorzystanie wzajemnej pomocy[26]. Mechanizm kompleksowej obsługi, który jest kluczowym atutem rynku wewnętrznego, jest wykorzystywany do rozstrzygania wielu spraw transgranicznych[27]. Obecnie trwają prace nad ważnymi decyzjami o wymiarze transgranicznym, które będą podlegać mechanizmowi kompleksowej obsługi. Decyzje te, dotyczące często wielonarodowych korporacji działających w sektorze zaawansowanych technologii, będą miały znaczny wpływ na prawa obywateli w wielu państwach członkowskich.

Rozwijanie prawdziwie wspólnej europejskiej kultury ochrony danych między organami ochrony danych jest jednak nadal procesem w toku. Organy ochrony danych nie wykorzystały jeszcze w pełni narzędzi przewidzianych w RODO, takich jak wspólne operacje, które mogą prowadzić do wspólnych dochodzeń. W niektórych przypadkach nie udało się osiągnąć wspólnego podejścia, które oznaczałoby przejście do najmniejszego wspólnego mianownika, a co za tym idzie – możliwości większej harmonizacji[28].

Konieczne są dalsze postępy prac, aby usprawnić i ujednolicić rozpatrywanie spraw transgranicznych w całej UE, w tym z proceduralnego punktu widzenia, na przykład w kwestiach takich jak procedury rozpatrywania skarg, kryteria dopuszczalności skarg, czas trwania postępowań w kontekście różnych ram czasowych lub brak odnośnych terminów w zakresie krajowego administracyjnego prawa procesowego, moment w postępowaniu, w którym przysługuje prawo do bycia wysłuchanym lub informacje i zaangażowanie skarżących w toku postępowania. Proces refleksji zainicjowany przez EROD w związku z powyższym został pozytywnie przyjęty, a Komisja bierze czynny udział w odnośnych dyskusjach[29].

Działania i wytyczne EROD mają kluczowe znaczenie dla dalszego spójnego rozwoju wymiany informacji między radą a zainteresowanymi stronami[30]. Do końca 2019 r. EROD przyjął 67 dokumentów, w tym 10 nowych wytycznych[31] oraz 43 opinii[32]. Zainteresowane strony zasadniczo z zadowoleniem przyjmują wytyczne EROD i zwracają się o dodatkowe wytyczne w odniesieniu do kluczowych pojęć zawartych

[25] Jeżeli dane przedsiębiorstwo przetwarza dane poza granicami jednego państwa, to właściwym organem ochrony danych jest jedno z państw członkowskich, w którym znajduje się główna siedziba spółki.
[26] Zob. pkt 2.2 dokumentu roboczego służb Komisji.
[27] W okresie od dnia 25 maja 2018 r. do dnia 31 grudnia 2019 r. w ramach procedury kompleksowej obsługi przedłożono 141 projektów decyzji, z czego 79 skutkowało wydaniem ostatecznych decyzji.
[28] Na przykład krajowe wykazy rodzajów operacji przetwarzania, które wymagają oceny skutków w zakresie ochrony danych na podstawie art. 35 RODO, mogłyby zostać bardziej zharmonizowane.
[29] Zob. pkt 2.2 dokumentu roboczego służb Komisji.
[30] W szczególności przedstawicielami przedsiębiorstw i społeczeństwa obywatelskiego. Zob. pkt 2.3 dokumentu roboczego służb Komisji.
[31] Są one uzupełnieniem 10 wytycznych przyjętych przez Grupę Roboczą Art. 29 w okresie poprzedzającym rozpoczęcie stosowania rozporządzenia i zatwierdzonych przez EROD. Między styczniem a końcem maja 2020 r. EROD przyjął również dodatkowe 4 wytyczne i dokonał aktualizacji istniejących wcześniej wytycznych.
[32] 42 z tych opinii przyjęto na podstawie art. 64 RODO, a jedna została przyjęta na podstawie art. 70 ust. 1 lit. s) RODO i dotyczyła decyzji stwierdzającej odpowiedni stopień ochrony w odniesieniu do Japonii.

w ogólnym rozporządzeniu o ochronie danych, ale również wskazują na niespójność między wytycznymi krajowymi a wytycznymi EROD. Podkreślają one potrzebę bardziej praktycznych porad, w szczególności bardziej konkretnych przykładów, oraz potrzebę wyposażenia organów ochrony danych w niezbędne zasoby ludzkie, techniczne i finansowe w celu skutecznego wykonywania ich zadań.

Komisja konsekwentnie podkreślała spoczywający na państwach członkowskich obowiązek przeznaczania wystarczających zasobów ludzkich, finansowych i technicznych na potrzeby krajowych organów ochrony danych[33]. Większość organów zanotowała wzrost liczby personelu i zwiększenie budżetu w latach 2016–2019[34], przy czym władze Irlandii, Niderlandów, Islandii, Luksemburga i Finlandii zanotowały największy względny wzrost liczby personelu. Ponieważ największe międzynarodowe korporacje technologiczne mają siedzibę w Irlandii i Luksemburgu, organy ochrony danych z tych państw działają jako organy wiodące w wielu ważnych sprawach transgranicznych i mogą potrzebować większych zasobów niż wynikałoby to z liczby ludności. Sytuacja jest jednak nadal nierówna między państwami członkowskimi i w ujęciu ogólnym nie można tego stanu uznać za zadowalający. Organy ochrony danych odgrywają zasadniczą rolę w zapewnieniu egzekwowania RODO na szczeblu krajowym oraz skutecznego funkcjonowania mechanizmów współpracy i spójności w ramach EROD, w tym w szczególności mechanizmu kompleksowej obsługi w sprawach transgranicznych. W związku z tym wzywa się państwa członkowskie do zapewnienia im odpowiednich zasobów zgodnie z wymogami RODO[35].

Zharmonizowane przepisy przy istniejącym wciąż pewnym stopniu rozdrobnieniu i rozbieżnych podejściach

Komisja monitoruje wdrażanie RODO w przepisach krajowych. W momencie sporządzania niniejszego sprawozdania wszystkie państwa członkowskie, z wyjątkiem Słowenii, przyjęły nowe przepisy lub dostosowały własne krajowe przepisy o ochronie danych. Słowenia[36] została poproszona o przedstawienie Komisji wyjaśnień dotyczących zakończenia tego procesu[37].

W ramach RODO przewidziano spójne podejście do przepisów o ochronie danych w całej UE. Rozporządzenie nakłada jednak na państwa członkowskie obowiązek stanowienia prawa w niektórych obszarach[38] i daje im możliwość dalszego doprecyzowania RODO[39]. W związku z tym nadal istnieje pewien stopień fragmentacji, który wynika w szczególności z szerokiego zastosowania opcjonalnych klauzul precyzujących. Na przykład różnice między państwami członkowskimi w zakresie wieku wyrażenia zgody przez dzieci w odniesieniu do usług społeczeństwa

[33] Komunikat Komisji do Parlamentu Europejskiego i Rady, „Przepisy dotyczące ochrony danych jako czynnik sprzyjający zaufaniu w UE i poza nią – podsumowanie", COM(2019) 374 final z 24.7.2019.
[34] W latach 2016–2019 odnotowano łączny wzrost liczby personelu o 42 % oraz wzrost budżetu krajowych organów ochrony danych w EOG o 49 %.
[35] Zob. pkt 2.4 dokumentu roboczego służb Komisji.
[36] W ostatnim czasie za pośrednictwem pisma komisarza Reyndersa w marcu 2020 r.
[37] Należy zauważyć, że krajowy organ ochrony danych w Słowenii został ustanowiony na podstawie obowiązującego krajowego prawa o ochronie danych i nadzoruje stosowanie RODO w tym państwie członkowskim.
[38] Zob. pkt 3.1 dokumentu roboczego służb Komisji.
[39] Zob. pkt 3.2 dokumentu roboczego służb Komisji.

informacyjnego powodują niepewność wśród dzieci i ich rodziców w kontekście stosowania ich praw w zakresie ochrony danych na jednolitym rynku. Ta fragmentacja stwarza również wyzwania dla prowadzenia działalności transgranicznej oraz innowacji, w szczególności w odniesieniu do nowych rozwiązań technologicznych i rozwiązań z zakresu cyberbezpieczeństwa. Aby zapewnić skuteczne funkcjonowanie rynku wewnętrznego i uniknąć niepotrzebnych obciążeń dla przedsiębiorstw, istotne jest również, aby przepisy krajowe nie wykraczały poza marginesy określone w RODO ani nie wprowadzały dodatkowych wymogów w przypadku braku marginesu.

Szczególnym wyzwaniem w odniesieniu do przepisów krajowych jest uzgodnienie prawa do ochrony danych osobowych z wolnością wypowiedzi i informacji oraz właściwe wyważenie tych praw. W niektórych przepisach krajowych ustanowiono zasadę pierwszeństwa wolności wypowiedzi, podczas gdy w innych pierwszeństwo ma ochrona danych osobowych, a przepisy o ochronie danych osobowych nie są stosowane wyłącznie w określonych sytuacjach, na przykład gdy chodzi o osobę o statusie osoby publicznej. Ponadto w innych państwach członkowskich prawodawca przewiduje pewne równoważenie praw lub ocenę poszczególnych przypadków w odniesieniu do odstępstw od niektórych przepisów RODO.

Komisja będzie nadal dokonywać oceny przepisów krajowych. Godzenie praw musi być przewidziane ustawą, szanować istotę praw podstawowych oraz być proporcjonalne i konieczne[40]. Przepisy dotyczące ochrony danych (jak również ich wykładnia i stosowanie) nie powinny mieć wpływu na korzystanie z prawa do wolności wypowiedzi i informacji, na przykład przez tworzenie efektu zniechęcającego lub wywieranie presji na dziennikarzy w celu ujawnienia ich źródeł. Wyważenie tych dwóch praw na mocy prawa krajowego powinno opierać się na orzecznictwie Trybunału Sprawiedliwości i Europejskiego Trybunału Praw Człowieka[41].

W przepisach państw członkowskich istnieją różne podejścia do wprowadzania odstępstw od ogólnego zakazu przetwarzania określonych kategorii danych osobowych, w odniesieniu do poziomu specyfikacji i zabezpieczeń, w tym do celów zdrowotnych i badawczych. W celu rozwiązania tej kwestii Komisja w pierwszej kolejności zidentyfikowała różne podejścia państw członkowskich[42] i w kolejnych krokach poprze ustanowienie kodeksów postępowania, które przyczyniłyby się do bardziej spójnego podejścia w tym obszarze oraz ułatwiły transgraniczne przetwarzanie danych osobowych.[43] Ponadto przyszłe wytyczne EROD w sprawie wykorzystywania danych osobowych w dziedzinie badań naukowych przyczynią się do zharmonizowanego podejścia. Komisja wniesie wkład do ustaleń EROD, w szczególności w odniesieniu do badań naukowych w dziedzinie zdrowia, w tym w formie konkretnych pytań i analizy scenariuszy, które otrzymała od środowiska naukowego.

[40] Art. 52 ust. 1 Karty.
[41] Zob. pkt 3.1 dokumentu roboczego służb Komisji: Godzenie prawa do ochrony danych osobowych z prawem do wolności wypowiedzi i informacji.
[42] Komisja rozpoczęła badanie dotyczące oceny przepisów państw członkowskich w dziedzinie danych w zakresie zdrowia w świetle RODO", Chafea/2018/Health/03, umowa szczegółowa nr 2019 70 01.
[43] Zob. działania zapowiedziane w europejskiej strategii w zakresie danych, s. 30.

Wzmocnienie pozycji osób fizycznych w zakresie kontrolowania ich danych

Według badania dotyczącego praw podstawowych[44] 69 % ludności UE w wieku powyżej 16 lat słyszało o RODO, a 71 % osób w UE wie o istnieniu krajowego organu ochrony danych.

Osoby fizyczne są coraz bardziej świadome swoich praw: prawa w zakresie dostępu do swoich danych osobowych, ich poprawiania, usuwania i przenoszenia, prawo do sprzeciwu wobec ich przetwarzania, jak również do większej przejrzystości. W ramach RODO wzmocniono prawa procesowe obejmujące prawo do złożenia skargi do organu ochrony danych, w tym poprzez powództwa przedstawicielskie, oraz prawo do dochodzenia roszczeń na drodze sądowej. Osoby fizyczne coraz częściej korzystają z tych praw, ale istnieje również potrzeba ułatwienia ich wykonywania i pełnego egzekwowania. Dyskusje prowadzone przez EROD pozwolą na wyjaśnienie i dalsze ułatwienie korzystania z praw indywidualnych, podczas gdy proponowana dyrektywa w sprawie powództw przedstawicielskich[45], po jej przyjęciu, ma umożliwić poszczególnym osobom wnoszenie powództw zbiorowych we wszystkich państwach członkowskich i obniżyć koszty działań transgranicznych.

Prawo do przenoszenia danych ma wyraźny potencjał, wciąż nie w pełni wykorzystywany, do umiejscowienia osób fizycznych w centrum gospodarki opartej na danych, umożliwiając im zmianę usługodawców, łączenie różnych usług, korzystanie z innych innowacyjnych usług oraz wybór usług najbardziej przyjaznych w kontekście ochrony danych. Będzie to pośrednio sprzyjać konkurencji i wspierać innowacje. Uwolnienie tego potencjału jest jednym z priorytetów Komisji, w szczególności dlatego, że coraz częściej korzysta się z urządzeń związanych z internetem rzeczy, a konsumenci generują coraz więcej danych, przy czym mogą oni zetknąć się ze stosowaniem nieuczciwych praktyk i efektem uzależnienia od dostawcy. Możliwość przenoszenia może przynieść istotne korzyści w odniesieniu do zdrowia i dobrobytu, zmniejszyć ślad środowiskowy i dostęp do usług publicznych i prywatnych, zwiększyć wydajność produkcji oraz podnieść jakość i bezpieczeństwo produktów.

W ramach strategii w zakresie danych podkreślono potrzebę rozwiązania problemów takich jak brak norm umożliwiających udostępnianie danych w formacie nadającym się do odczytu maszynowego w celu zwiększenia możliwości rzeczywistego korzystania z prawa do przenoszenia danych, które jest obecnie ograniczone do kilku sektorów (np. bankowości i telekomunikacji). Można to osiągnąć przede wszystkim przez opracowanie odpowiednich narzędzi, znormalizowanego formatu i interfejsów[46]. Korzystanie w większym stopniu z tego prawa można by również osiągnąć dzięki wprowadzeniu interfejsów technicznych i formatów nadających się do odczytu maszynowego umożliwiających przenoszenie danych w czasie rzeczywistym. Zwiększone korzystanie z prawa do przenoszenia danych może między

[44] Agencja Praw Podstawowych Unii Europejskiej (FRA) (2020): ankieta dot. praw podstawowych z 2019 r. Ochrona danych i technologia: https://fra.europa.eu/en/publication/2020/fundamental-rights-survey-data-protection.

[45] Oczekuje się, że proponowana dyrektywa w sprawie powództw przedstawicielskich w celu ochrony zbiorowych interesów konsumentów (COM(2018) 184 final – 2018/089 (COD)), po jej przyjęciu, wzmocni ramy powództw przedstawicielskich również w dziedzinie ochrony danych.

[46] Może to obejmować m.in. narzędzia zarządzania zgodą oraz aplikacje zarządzania danymi osobowymi.

innymi ułatwić osobom fizycznym udostępnianie ich danych dla dobra publicznego (na przykład w celu wspierania badań w sektorze zdrowia), jeśli sobie tego życzą („altruistyczne podejście do danych"). W ramach przygotowywania pakietu dotyczącego usług cyfrowych[47] Komisja zbada szerzej rolę danych i praktyk związanych z danymi w ekosystemie platform.

[47] https://ec.europa.eu/commission/presscorner/detail/pl/ip_20_962

Możliwości i wyzwania dla organizacji, w szczególności dla małych i średnich przedsiębiorstw

RODO wraz z rozporządzeniem w sprawie ram swobodnego przepływu danych nieosobowych[48] oferuje przedsiębiorstwom możliwości w zakresie wspierania konkurencji i innowacji, zapewnienia swobodnego przepływu danych w UE oraz stworzenia równych warunków działania dla przedsiębiorstw mających siedzibę poza UE[49]. Prawo do przenoszenia danych, w połączeniu z rosnącą liczbą osób poszukujących rozwiązań bardziej sprzyjających ochronie prywatności, może zmniejszyć bariery wejścia na rynek dla przedsiębiorstw i otworzyć możliwości wzrostu w oparciu o zaufanie i innowacje. Niektóre zainteresowane strony informują, że stosowanie RODO stanowi wyzwanie zwłaszcza dla małych i średnich przedsiębiorstw (MŚP). Zgodnie z podejściem opartym na analizie ryzyka przyznawanie odstępstw na podstawie wielkości operatorów nie byłoby podejściem właściwym, ponieważ ich rozmiar sam w sobie nie stanowi wskaźnika ryzyka, jakie przetwarzanie danych osobowych, którego to przedsiębiorstwo się podejmuje, może stworzyć dla osób fizycznych. Kilka organów ochrony danych dostarczyło praktyczne narzędzia ułatwiających wdrożenie RODO przez MŚP prowadzące działalność w zakresie przetwarzania o niskim ryzyku. Wysiłki te powinny zostać zintensyfikowane i rozpowszechnione, najlepiej w ramach wspólnego europejskiego podejścia, aby nie tworzyć barier dla jednolitego rynku.

Organy ochrony danych opracowały szereg działań mających pomóc MŚP w przestrzeganiu przepisów ogólnego rozporządzenia o ochronie danych, na przykład przez udostępnienie szablonów i zapisów dotyczących czynności przetwarzania, a także seminariów i gorących linii przeznaczonych do konsultacji. Wiele z tych inicjatyw skorzystało z finansowania UE[50]. Należy rozważyć dalsze działania mające na celu ułatwienie stosowania RODO w odniesieniu do MŚP.

RODO udostępnia zestaw narzędzi wszystkim rodzajom przedsiębiorstw i organizacji, aby pomóc im w wykazaniu zgodności, takich jak kodeksy postępowania, mechanizmy certyfikacji i standardowe klauzule umowne. Należy w pełni wykorzystywać ten zestaw narzędzi. MŚP podkreślają w szczególności znaczenie i użyteczność kodeksów postępowania dostosowanych do ich sytuacji i niepowodujących niewspółmiernych kosztów. W odniesieniu do systemów certyfikacji bezpieczeństwo (w tym cyberbezpieczeństwo) i ochrona danych w fazie projektowania są kluczowymi elementami, które należy uwzględnić w RODO i które skorzystałyby na wspólnym i ambitnym podejściu w całej UE. Komisja pracuje

[48] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1807 z dnia 14 listopada 2018 r. w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej, Dz.U. L 303 z 28.11.2018, s. 59.

[49] Zob. pkt 5 dokumentu roboczego służb Komisji. Zob. również COM(2019) 250 final, Wytyczne dotyczące rozporządzenia w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej, wyjaśniające zasady regulujące przetwarzanie mieszanych zbiorów danych, składających się zarówno z danych osobowych, jak i nieosobowych, i zawierające praktyczne rozwiązania dla przedsiębiorstw, w tym dla MŚP.

[50] Komisja udzieliła wsparcia finansowego w postaci trzech fal dotacji, na łączną kwotę 5 mln EUR, przy czym dwie ostatnie są przeznaczone specjalnie na wspieranie krajowych organów ochrony danych w wysiłkach na rzecz dotarcia do osób fizycznych oraz małych i średnich przedsiębiorstw: https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules/eu-funding-supporting-implementation-gdpr_pl. Dodatkowa kwota w wysokości 1 mln EUR zostanie przydzielona w 2020 r.

obecnie nad standardowymi klauzulami umownymi między administratorami a podmiotami przetwarzającymi[51], opierając się na trwających pracach nad modernizacją standardowych klauzul umownych dotyczących przekazywania za granicę[52].

Stosowanie RODO w kontekście nowych technologii

Jako opracowane w sposób neutralny pod względem technicznym RODO opiera się na zasadach i w związku z tym jest może uwzględniać nowe technologie w miarę ich rozwoju.

Rozporządzenie jest postrzegane jako niezbędne i elastyczne narzędzie gwarantujące, że rozwój nowych technologii jest zgodny z prawami podstawowymi. Ramy prawne dotyczące ochrony danych i prywatności dowiodły swej wagi i elastyczności podczas kryzysu związanego z emisją COVID-19, w szczególności w odniesieniu do projektowania aplikacji do śledzenia kontaktów i innych rozwiązań technologicznych mających na celu zwalczanie pandemii. Przyszłe wyzwania wiążą się z potrzebą wyjaśnienia sposobu stosowania sprawdzonych zasad do konkretnych technologii, takich jak sztuczna inteligencja, łańcuch bloków, internet rzeczy lub rozpoznawanie twarzy, które wymagają ciągłego monitorowania. Na przykład biała księga Komisji w sprawie sztucznej inteligencji[53] otworzyła debatę publiczną na temat konkretnych okoliczności, które mogłyby uzasadniać wykorzystanie sztucznej inteligencji do celów zdalnej identyfikacji biometrycznej (np. rozpoznawania twarzy) w miejscach publicznych, oraz na temat ogólnych zabezpieczeń. W związku z tym organy ochrony danych powinny być zawczasu gotowe do udziału w projektowaniu technicznym.

Ponadto zasadniczym elementem ochrony osób fizycznych jest zdecydowane i skuteczne egzekwowanie RODO w odniesieniu do dużych platform cyfrowych i zintegrowanych przedsiębiorstw, w tym w takich obszarach jak reklama internetowa i mikrotargetowanie.

Opracowanie nowoczesnego międzynarodowego zestawu narzędzi do przekazywania danych

W ramach RODO przewidziano unowocześniony zestaw narzędzi ułatwiających przekazywanie danych osobowych z UE do państw trzecich lub organizacji międzynarodowych, przy jednoczesnym zapewnieniu dalszego korzystania z wysokiego poziomu ochrony danych. W ciągu ostatnich dwóch lat Komisja zintensyfikowała prace mające na celu wykorzystanie pełnego potencjału narzędzi dostępnych w ramach RODO.

Prace te polegały m.in. na aktywnej współpracy z kluczowymi partnerami w celu wydania „decyzji stwierdzającej odpowiedni stopień ochrony. Wskutek takiej decyzji możliwy staje się bezpieczny swobodny przepływ danych osobowych do danego państwa trzeciego bez potrzeby przedstawiania dodatkowych gwarancji przez podmiot przekazujący dane lub uzyskania przez niego odpowiedniego upoważnienia. W szczególności wzajemne decyzje stwierdzające odpowiedni stopień ochrony

[51] Zgodnie z art. 28 RODO.
[52] Zgodnie z art. 46 RODO.
[53] Biała księga w sprawie sztucznej inteligencji – Europejskie podejście do doskonałości i zaufania – COM(2020) 65 final.

przyjęte przez UE i Japonię, które weszły w życie w lutym 2019 r., stworzyły największy na świecie obszar wolnych i bezpiecznych przepływów danych. Ponadto proces związany z decyzjami stwierdzającymi odpowiedni stopień ochrony w stosunku do Republiki Korei jest na zaawansowanym etapie i prowadzone są rozmowy wstępne z innymi ważnymi partnerami w Azji i Ameryce Łacińskiej.

Stwierdzenie odpowiedniego stopnia ochrony odgrywa również ważną rolę w kontekście przyszłych stosunków ze Zjednoczonym Królestwem, pod warunkiem że spełnione są odpowiednie warunki. Stanowi on czynnik wspomagający handel, w tym cyfrowy, i jest niezbędnym warunkiem ścisłej i ambitnej współpracy w dziedzinie egzekwowania prawa i bezpieczeństwa. Ponadto wysoki stopień konwergencji w zakresie ochrony danych jest ważnym elementem zapewnienia równych warunków działania między dwiema tak ściśle zintegrowanymi gospodarkami. Zgodnie z deklaracją polityczną w sprawie przyszłych stosunków między UE a Zjednoczonym Królestwem Komisja prowadzi obecnie ocenę stopnia ochrony na podstawie zarówno RODO, jak i dyrektywy o ochronie danych w sprawach karnych[54].

W ramach pierwszej oceny RODO Komisja jest również zobowiązana do dokonania przeglądu decyzji stwierdzających odpowiedni stopień ochrony, które zostały przyjęte na mocy poprzednich przepisów[55]. Służby Komisji zaangażowały się w intensywny dialog z każdym z 11 zainteresowanych państw trzecich i terytoriów[56] w celu dokonania oceny rozwoju ich systemów ochrony danych od czasu przyjęcia decyzji stwierdzającej odpowiedni stopień ochrony oraz tego, czy spełniają one standardy określone w RODO. Potrzeba zapewnienia ciągłości takich decyzji – kluczowego narzędzia handlu i współpracy międzynarodowej – jest jednym z czynników, które skłoniły kilka z tych państw i terytoriów do modernizacji i wzmocnienia ich prawa w zakresie ochrony prywatności. Z niektórymi z tych państw i terytoriów omawiane są dodatkowe zabezpieczenia w celu wyeliminowania istotnych różnic w zakresie ochrony. Biorąc jednak pod uwagę fakt, że Trybunał Sprawiedliwości w wyroku, który ma zostać wydany w dniu 16 lipca, może przedstawić wyjaśnienia, które mogą mieć znaczenie dla niektórych elementów normy dotyczącej odpowiedniego stopnia ochrony, Komisja przedstawi oddzielnie sprawozdanie na temat oceny istniejących orzeczeń w sprawie odpowiedniej ochrony danych osobowych po wydaniu przez Trybunał Sprawiedliwości wyroku w tej sprawie[57].

---

[54] 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, Dz.U. L 119 z 4.5.2016, s. 89.

[55] 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.

[56] Te państwa i terytoria to: Andora, Argentyna, Kanada, Wyspy Owcze, Guernsey, Jersey, Wyspa Man, Izrael, Nowa Zelandia, Szwajcaria i Urugwaj.

[57] Zob. sprawa C-311/18 Data Protection Commissioner przeciwko Facebook Ireland Limited, Maximillian Schrems („Schrems II"), która dotyczy orzeczenia w trybie prejudycjalnym dotyczącego tzw. standardowych klauzul umownych. Trybunał może jednak również doprecyzować niektóre elementy normy dotyczącej odpowiedniego stopnia ochrony.

Oprócz prac w zakresie odpowiedniego stopnia ochrony Komisja pracuje nad kompleksową modernizacją standardowych klauzul umownych w celu ich zaktualizowania w świetle nowych wymogów wprowadzonych na mocy RODO. Celem tych prac jest lepsze odzwierciedlenie realiów operacji przetwarzania w nowoczesnej gospodarce cyfrowej i rozważenie ewentualnej potrzeby dalszego sprecyzowania pewnych zabezpieczeń, w tym z uwzględnieniem przyszłego orzecznictwa Trybunału Sprawiedliwości[58]. Klauzule te stanowią zdecydowanie najbardziej rozpowszechnioną metodę przekazywania danych, co znajduje odzwierciedlenie w fakcie, że tysiące przedsiębiorstw unijnych bazuje na nich w celu świadczenia szerokiego zakresu usług na rzecz swoich klientów, dostawców, partnerów i pracowników.

EROD odegrał również aktywną rolę w opracowywaniu międzynarodowych aspektów RODO, która obejmowała m.in. aktualizację wytycznych dotyczących istniejących mechanizmów przekazywania danych, takich jak wiążące reguły korporacyjne i tzw. „odstępstwa", a także rozwój infrastruktury prawnej na potrzeby stosowania nowych narzędzi wprowadzonych na mocy RODO, tj. kodeksów postępowania i certyfikacji.

Aby umożliwić zainteresowanym stronom pełne korzystanie z zestawu narzędzi RODO, ważne jest, aby EROD zintensyfikował prace nad różnymi mechanizmami przekazywania danych, w tym przez dalsze usprawnianie procesu zatwierdzania wiążących reguł korporacyjnych, sfinalizowanie wytycznych dotyczących kodeksów postępowania i certyfikacji jako narzędzi przekazywania danych oraz wyjaśnienie powiązań między przepisami dotyczącymi przekazywania danych za granicę (rozdział V) a terytorialnym zakresem stosowania RODO (art. 3).

Innym ważnym aspektem międzynarodowego wymiaru przepisów UE dotyczących ochrony danych jest rozszerzony zakres terytorialny ogólnego rozporządzenia o ochronie danych, który obejmuje również działania podmiotów zagranicznych prowadzących działalność w zakresie przetwarzania danych na rynku UE. Odpowiednie uwzględnienie tego rozszerzenia w działaniach organów ochrony danych dotyczących egzekwowania prawa ma zasadnicze znaczenie dla zapewnienia faktycznego przestrzegania RODO i prawdziwie równych warunków działania. Organy te powinny w szczególności nawiązać współpracę, w razie konieczności, z przedstawicielem administratora danych lub podmiotu przetwarzającego w UE, do którego można zwracać się w uzupełnieniu lub zamiast do przedsiębiorstwa mającego siedzibę poza UE. Podejście to powinno być energicznie realizowane w celu wysłania wyraźnej wiadomości, że brak siedziby w UE nie zwalnia zagranicznych podmiotów z obowiązków wynikających z RODO.

Wspieranie konwergencji i międzynarodowej współpracy w dziedzinie ochrony danych

RODO stało się już kluczowym punktem odniesienia na szczeblu międzynarodowym i stanowiło katalizator dla wielu krajów na świecie, aby rozważyć wprowadzenie nowoczesnych przepisów dotyczących prywatności. Ta tendencja w kierunku globalnej konwergencji jest bardzo pozytywnym zjawiskiem, które stwarza nowe

[58] Zob. sprawa Schrems II.

możliwości lepszej ochrony osób fizycznych w UE, gdy ich dane są przekazywane za granicę, a jednocześnie ułatwia przepływ danych.

W oparciu o tę tendencję Komisja zintensyfikowała dialog na wielu forach dwustronnych, regionalnych i wielostronnych, aby wspierać globalną kulturę poszanowania prywatności i opracować elementy konwergencji między różnymi systemami ochrony prywatności. W swoich wysiłkach Komisja powołała się na aktywne wsparcie Europejskiej Służby Działań Zewnętrznych i sieci delegatur UE w państwach trzecich oraz misji przy organizacjach międzynarodowych i zamierza również powoływać się na nie w przyszłości. Pozwoliło to również osiągnąć większą spójność i komplementarność różnych aspektów zewnętrznego wymiaru polityki UE – od handlu do nowego partnerstwa między UE a Afryką. Grupa G20 i grupa G7 również doceniły niedawno wkład ochrony danych w zaufanie do gospodarki cyfrowej i przepływów danych, w szczególności poprzez koncepcję „Data Free Flow with Trust" (ang. „swobodny przepływ danych oparty na zaufaniu"), którą pierwotnie zaproponowała japońska prezydencja G20.[59] Strategia w zakresie danych podkreśla, że Komisja zamierza nadal promować wymianę danych z zaufanymi partnerami, a jednocześnie zwalczać nadużycia, takie jak nieproporcjonalny dostęp (zagranicznych) organów publicznych do danych osobowych.

Propagując konwergencję standardów ochrony danych na szczeblu międzynarodowym, jako sposób na ułatwienie przepływu danych, a co za tym idzie, na wymianę handlową, Komisja jest również zdecydowana przeciwdziałać protekcjonizmowi cyfrowemu, co zostało niedawno podkreślone w ramach strategii w zakresie danych.[60] W tym celu opracowała szczegółowe przepisy dotyczące przepływu danych i ochrony danych w umowach handlowych[61], które systematycznie uwzględnia w umowach dwustronnych – ostatnio z Australią, Nową Zelandią i Zjednoczonym Królestwem – oraz negocjacjach wielostronnych, takich jak obecne rozmowy w ramach WTO w sprawie handlu elektronicznego[62]. Te przepisy horyzontalne wykluczają nieuzasadnione ograniczenia, takie jak przymusowe wymogi dotyczące lokalizacji danych, a z drugiej strony zachowują autonomię regulacyjną stron w zakresie ochrony podstawowego prawa do ochrony danych.

Należy zatem dalej badać możliwości synergii między instrumentami ochrony handlu i danych w celu zapewnienia swobodnego i bezpiecznego międzynarodowego przepływu danych, który ma zasadnicze znaczenie dla działalności gospodarczej, konkurencyjności i rozwoju europejskich przedsiębiorstw, w tym MŚP, w coraz bardziej cyfrowej gospodarce.

---

[59] Zob. np. treść deklaracji przywódców grupy G20: https://www.consilium.europa.eu/media/40124/final_g20_osaka_leaders_declaration.pdf.

[60] Strategia w zakresie danych, s. 23.

[61] Zob. tekst przepisów horyzontalnych dotyczących transgranicznych przepływów danych i ochrony danych osobowych (w unijnych umowach handlowych i inwestycyjnych): https://trade.ec.europa.eu/doclib/docs/2018/may/tradoc_156884.pdf.

[62] 84 członków WTO jest obecnie zaangażowanych w wielostronne negocjacje w sprawie handlu elektronicznego w związku ze wspólną deklaracją przyjętą przez ministrów w dniu 25 stycznia 2019 r. w Davos. W ramach tego procesu UE przedłożyła 3 maja 2019 r. tekst wniosku w sprawie przyszłych przepisów i obowiązków w zakresie handlu elektronicznego. Wniosek zawiera przepisy horyzontalne dotyczące przepływu danych i ochrony danych osobowych: https://trade.ec.europa.eu/doclib/docs/2019/may/tradoc_157880.pdf.

Podobnie ważne jest zagwarantowanie, aby w przypadku gdy przedsiębiorstwa działające na rynku europejskim zostaną wezwane na podstawie uzasadnionego wniosku o udostępnienie danych do celów egzekwowania prawa, mogły tego dokonać bez ryzyka kolizji przepisów i przy pełnym poszanowaniu praw podstawowych UE. Aby usprawnić takie przekazywanie danych, Komisja zobowiązuje się do opracowania odpowiednich ram prawnych z partnerami międzynarodowymi w celu unikania kolizji przepisów i wspierania efektywnych form współpracy, zwłaszcza przez zapewnienie niezbędnych zabezpieczeń w zakresie ochrony danych, a tym samym przyczynienia się do skuteczniejszej walki z przestępczością.

Ponadto w sytuacjach, w których kwestie związane z przestrzeganiem prawa do prywatności lub incydenty związane z bezpieczeństwem danych mogą mieć wpływ na dużą liczbę osób w kilku jurysdykcjach jednocześnie, należy jeszcze bardziej zacieśnić współpracę w terenie między europejskimi i międzynarodowymi organami regulacyjnymi. Wymaga to w szczególności opracowania odpowiednich instrumentów prawnych w celu zacieśnienia współpracy i wzajemnej pomocy, w tym przez umożliwienie niezbędnej wymiany informacji w kontekście dochodzeń. W tym właśnie duchu Komisja powołuje Akademię Ochrony Danych (Data Protection Academy), platformę, w ramach której unijne i zagraniczne organy ochrony danych dzielą się wiedzą, doświadczeniem i najlepszymi praktykami w celu ułatwienia i wspierania współpracy między organami odpowiedzialnymi za egzekwowanie prawa w zakresie ochrony prywatności.

3 DALSZE DZIAŁANIA

Aby w pełni zrealizować potencjał RODO, ważne jest stworzenie zharmonizowanego podejścia i wspólnej europejskiej kultury ochrony danych oraz wspieranie bardziej skutecznego i zharmonizowanego postępowania w sprawach transgranicznych. Jest to zgodne z oczekiwaniami ludzi i przedsiębiorstw oraz stanowi zasadniczy cel reformy unijnych przepisów o ochronie danych. Równie ważne jest zagwarantowanie, aby wszystkie narzędzia dostępne w RODO były w pełni wykorzystywane w celu zapewnienia skutecznego stosowania tego rozporządzenia w odniesieniu do osób fizycznych i przedsiębiorstw.

Komisja będzie kontynuować dwustronną wymianę informacji z państwami członkowskimi na temat wdrażania RODO i, w razie potrzeby, będzie nadal wykorzystywać wszystkie dostępne narzędzia do zapewnienia przestrzegania przez państwa członkowskie zobowiązań wynikających z RODO.

Biorąc pod uwagę ciągłą ocenę przepisów krajowych, krótki okres praktycznego stosowania przepisów RODO oraz fakt, że w wielu państwach członkowskich prawodawstwo sektorowe jest wciąż poddawane przeglądowi, wyciąganie ostatecznych wniosków na temat obecnego poziomu fragmentacji byłoby przedwczesne. W kontekście ewentualnej kolizji przepisów w związku z wdrożeniem przez państwa członkowskie klauzul precyzujących należy najpierw lepiej zrozumieć konsekwencje dla administratorów danych i podmiotów przetwarzających[63].

[63] Zob. stanowisko Rady i ustalenia w sprawie stosowania RODO.

Podejmując działania następcze w związku z tymi kwestiami, można odwoływać się do stosownego orzecznictwa sądów krajowych i Trybunału Sprawiedliwości, które przyczynia się do stworzenia spójnej wykładni przepisów o ochronie danych. Sądy krajowe wydały ostatnio wyroki w sprawie unieważnienia przepisów prawa krajowego, które odbiegają od przepisów RODO[64].

W wymiarze międzynarodowym Komisja będzie nadal koncentrować się na wspieraniu konwergencji przepisów o ochronie danych w celu zapewnienia bezpiecznego przepływu danych. Dotyczy to różnych form pracy proaktywnej, na przykład w kontekście trwających reform w zakresie nowych lub zaktualizowanych przepisów o ochronie danych lub dążenia do koncepcji „swobodnego przepływu danych opartego na zaufaniu" na forach wielostronnych. Powyższe działania obejmują również różne dialogi dotyczące odpowiedniego stopnia ochrony oraz modernizację i rozbudowę naszego zestawu narzędzi do przekazywania danych przez aktualizację standardowych klauzul umownych i stworzenie podstaw mechanizmów certyfikacji. Prace te obejmują również negocjacje międzynarodowe, np. w dziedzinie transgranicznego dostępu do dowodów elektronicznych, w celu zagwarantowania, by przekazywanie danych odbywało się przy zastosowaniu odpowiednich zabezpieczeń w zakresie ochrony danych. Wreszcie, angażując się w negocjacje w sprawie współpracy międzynarodowej i wzajemnej pomocy między organami odpowiedzialnymi za egzekwowanie przepisów w zakresie ochrony danych, Komisja będzie dążyć do konwergencji przepisów w tym obszarze.

Na podstawie tej oceny stosowania RODO od maja 2018 r. wymienione poniżej działania zostały uznane za konieczne do wspierania jego stosowania. Komisja będzie monitorować ich wdrażanie również w kontekście zbliżającego się sprawozdania z oceny w 2024 r.

Wdrażanie i uzupełnianie ram prawnych

Państwa członkowskie powinny:

- zakończyć proces dostosowywania własnych przepisów sektorowych do przepisów RODO;
- rozważyć ograniczenie stosowania klauzul precyzujących, które mogłyby prowadzić do fragmentacji i zagrozić swobodnemu przepływowi danych w UE;
- ocenić, czy krajowe przepisy wdrażające RODO przewidują wszystkie okoliczności w ramach marginesu przewidzianego dla przepisów państwa członkowskiego.

Komisja będzie:

- prowadzić dwustronną wymianę z państwami członkowskimi na temat zgodności przepisów krajowych z RODO, w tym na temat niezależności i zasobów krajowych organów ochrony danych; wykorzystywać wszystkie dostępne narzędzia, w tym postępowania w sprawie uchybienia

[64] Tak było w przypadku Niemiec, Hiszpanii i Austrii, a wyroki te pozwoliły wypełnić luki w przepisach krajowych.

zobowiązaniom państwa członkowskiego, w celu zagwarantowania, by państwa członkowskie przestrzegały RODO;

- wspierać dalszą wymianę poglądów i praktyk krajowych między państwami członkowskimi na tematy, które podlegają dalszemu doprecyzowaniu na szczeblu krajowym, w celu zredukowania stopnia fragmentacji jednolitego rynku, takie jak przetwarzanie danych osobowych związane ze zdrowiem i badaniami, lub które należy równoważyć z innymi prawami, takimi jak wolność wypowiedzi;
- zapewniać spójne stosowanie ram ochrony danych w odniesieniu do nowych technologii w celu wspierania innowacji i rozwoju technologicznego;
- wykorzystywać wysiłki grupy ekspertów ds. RODO z państw członkowskich (ustanowionej na etapie przejściowym przed wejściem rozporządzenia w życie) w celu ułatwienia dyskusji i wymiany doświadczeń między państwami członkowskimi i z Komisją;
- badać, czy – w świetle dalszych doświadczeń i stosownego orzecznictwa – zaproponowanie ewentualnych przyszłych ukierunkowanych zmian w niektórych przepisach RODO może być właściwe, w szczególności w odniesieniu do dokumentacji dotyczącej przetwarzania danych przez MŚP, które nie przetwarzają danych osobowych w ramach podstawowej działalności (niskie ryzyko)[65], oraz ewentualnej harmonizacji wieku wyrażenia zgody przez dzieci w zakresie świadczenia usług społeczeństwa informacyjnego.

Pełne wykorzystanie potencjału nowego systemu zarządzania

EROD oraz organy ochrony danych wzywa się do:

- opracowania skutecznych rozwiązań między organami ochrony danych dotyczących funkcjonowania mechanizmu współpracy i spójności, w tym aspektów proceduralnych, w oparciu o wiedzę fachową ich członków oraz przez zwiększenie zaangażowania sekretariatu;
- wspierania harmonizacji stosowania i egzekwowania przepisów RODO przy użyciu wszelkich dostępnych środków, w tym przez dalsze doprecyzowanie kluczowych pojęć RODO, oraz zagwarantowanie, by krajowe wytyczne były w pełni zgodne z wytycznymi przyjętymi przez EROD;
- zachęcania do stosowania wszystkich narzędzi przewidzianych w przepisach RODO w celu zapewnienia ich spójnego stosowania;
- zacieśniania współpracy między organami ochrony danych, na przykład przez prowadzenie wspólnych dochodzeń.

Komisja będzie:

- nadal ściśle monitorować efektywną i pełną niezależność krajowych organów ochrony danych;

[65] Art. 30 ust. 5 RODO.

- zachęcać do współpracy między organami regulacyjnymi (w szczególności w takich obszarach jak konkurencja, łączność elektroniczna, bezpieczeństwo sieci i systemów informatycznych oraz polityka konsumencka);
- sprzyjać podejmowaniu odpowiednich działań przez EROD w kontekście procedur stosowanych przez krajowe organy ochrony danych w celu poprawy współpracy w sprawach transgranicznych.

Państwa członkowskie powinny

- przydzielać zasoby organom ochrony danych wystarczające do wykonywania ich zadań.

Wspieranie zainteresowanych stron

EROD oraz organy ochrony danych wzywa się do:

- przyjmowania dalszych praktycznych, łatwych do zrozumienia wytycznych, które dostarczają jasnych odpowiedzi i pozwalają uniknąć niejednoznaczności w kwestiach związanych ze stosowaniem RODO, na przykład w odniesieniu do przetwarzania danych dzieci i osób, których dane dotyczą, w tym do korzystania z prawa do dostępu i prawa do usunięcia danych, z zainteresowanymi stronami uczestniczącymi w tym procesie;
- dokonywania przeglądu wytycznych w przypadku, gdy konieczne są dalsze wyjaśnienia w świetle doświadczeń i zmian, w tym w orzecznictwie Trybunału Sprawiedliwości;
- opracowania praktycznych narzędzi, takich jak zharmonizowane formularze na potrzeby naruszeń ochrony danych oraz uproszczone rejestry działań związanych z przetwarzaniem, aby pomóc małym i średnim przedsiębiorstwom o niskim poziomie ryzyka w wypełnianiu ich obowiązków.

Komisja będzie:

- zapewniać standardowe klauzule umowne zarówno w odniesieniu do przekazywania danych za granicę, jak i relacji między administratorem danych a podmiotem przetwarzającym;
- zapewniać narzędzia wyjaśniające/wspierające stosowanie przepisów o ochronie danych w odniesieniu do dzieci[66];
- zgodnie ze strategią w zakresie danych, badać praktyczne środki ułatwiające szerszy zakres korzystania z prawa do przenoszenia danych przez osoby fizyczne, takie jak zapewnienie im większej kontroli nad tym, kto może uzyskać dostęp do maszynowo generowanych danych i je wykorzystywać;
- wspierać standaryzację/certyfikację, w szczególności w odniesieniu do aspektów cyberbezpieczeństwa, poprzez współpracę między Agencją Unii

[66] Projekt Komisji w sprawie narzędzi identyfikacji wieku – projekt pilotażowy w celu zademonstrowania interoperacyjnej infrastruktury technicznej w zakresie ochrony dzieci, w tym weryfikacji wieku i zgody rodziców. Oczekuje się, że przyczyni się to do wdrożenia mechanizmów ochrony dzieci w oparciu o istniejące przepisy UE dotyczące ochrony dzieci w internecie.

Europejskiej ds. Cyberbezpieczeństwa (ENISA), organami ochrony danych i EROD;

- w stosownych przypadkach, korzystać z prawa do zwrócenia się do EROD o przygotowanie wytycznych i opinii na temat konkretnych kwestii istotnych dla zainteresowanych stron;
- w razie potrzeby, określać wytyczne, przy pełnym poszanowaniu roli EROD;
- wspierać działania organów ochrony danych, które ułatwiają MŚP wypełnianie obowiązków wynikających z RODO, poprzez wsparcie finansowe, w szczególności w zakresie praktycznych wytycznych i narzędzi cyfrowych, które mogą być powielane w innych państwach członkowskich.

Zachęcanie do nowatorstwa

Komisja będzie:

- monitorować stosowanie przepisów RODO w odniesieniu do nowych technologii, uwzględniając również ewentualne przyszłe inicjatywy w obszarze sztucznej inteligencji i w ramach strategii w zakresie danych;
- zachęcać, w tym poprzez wsparcie finansowe, do opracowywania unijnych kodeksów postępowania w dziedzinie zdrowia i badań naukowych;
- uważnie śledzić rozwój i stosowanie aplikacji w kontekście pandemii COVID-19.

EROD wzywa się do:

- wydawania wytycznych w sprawie stosowania RODO w obszarze badań naukowych, sztucznej inteligencji, łańcucha bloków i ewentualnych innych rozwiązań technologicznych;
- dokonywania przeglądu wytycznych, w przypadku gdy konieczne są dalsze wyjaśnienia w kontekście rozwoju technologicznego.

Dalszy rozwój zestawu narzędzi służących do przekazywania danych

Komisja będzie:

- prowadzić dialog na temat odpowiedniej ochrony danych osobowych z zainteresowanymi państwami trzecimi, zgodnie ze strategią określoną w komunikacie z 2017 r. pt. „Wymiana i ochrona danych osobowych w zglobalizowanym świecie", w tym, w miarę możliwości, uwzględniając przekazywanie danych organom ścigania (na mocy dyrektywy o ochronie danych w sprawach karnych) i innym organom publicznym; obejmuje to również finalizację procesu stwierdzenie odpowiedniego stopnia ochrony w odniesieniu do Republiki Korei tak szybko, jak to możliwe;
- odpowiedzialna za finalizację trwającej oceny istniejących decyzji stwierdzających odpowiedni stopień ochrony danych osobowych i złożenie sprawozdań Parlamentowi Europejskiemu i Radzie;
- odpowiedzialna za finalizację prac nad modernizacją standardowych klauzul umownych – w celu ich aktualizacji w świetle ogólnego rozporządzenia

o ochronie danych – obejmujących wszystkie istotne scenariusze przekazywania i lepiej odzwierciedlających nowoczesne praktyki biznesowe.

EROD wzywa się do:

- dalszego doprecyzowania powiązań między przepisami dotyczącymi przekazywania danych za granicę (rozdział V) a terytorialnym zakresem stosowania RODO (art. 3);
- zapewnienia skutecznego egzekwowania przepisów w odniesieniu do podmiotów mających siedzibę w państwach trzecich objętych zakresem terytorialnym RODO, w tym w odniesieniu do wyznaczenia przedstawiciela, w stosownych przypadkach (art. 27);
- usprawnienia oceny i ostatecznego zatwierdzenia wiążących reguł korporacyjnych w celu przyspieszenia procesu;
- zakończenia prac nad strukturą, procedurami i kryteriami oceny w odniesieniu do kodeksów postępowania i mechanizmów certyfikacji jako narzędzi przekazywania danych.

Promowanie konwergencji i rozwijanie współpracy międzynarodowej

Komisja będzie:

- wspierać trwające procesy reform w państwach trzecich w zakresie nowych lub zmodernizowanych przepisów o ochronie danych przez dzielenie się doświadczeniami i najlepszymi praktykami;
- współpracować z partnerami z Afryki w celu promowania konwergencji regulacyjnej i wspierania budowania zdolności organów nadzorczych w ramach rozdziału cyfrowego nowego partnerstwa między UE a Afryką;
- prowadzić ocenę możliwości ułatwienia współpracy między podmiotami prywatnymi a organami ścigania, w tym przez negocjowanie dwustronnych i wielostronnych ram przekazywania danych w kontekście dostępu zagranicznych organów ścigania do dowodów elektronicznych, aby uniknąć kolizji przepisów przy jednoczesnym zapewnieniu odpowiednich zabezpieczeń w zakresie ochrony danych;
- współpracować z organizacjami międzynarodowymi i regionalnymi, takimi jak OECD, ASEAN lub grupa G-20, w celu wspierania zaufanych przepływów danych w oparciu o wysokie standardy ochrony danych, w tym w kontekście inicjatywy „Data Free Flow with Trust”;
- odpowiedzialna za utworzenie Akademii Ochrony Danych w celu ułatwienia i wspierania przekazywania danych między europejskimi i międzynarodowymi organami regulacyjnymi;
- wspierać międzynarodową współpracę w zakresie egzekwowania prawa między organami nadzoru, w tym przez negocjowanie umów o współpracy i wzajemnej pomocy.